世界数学



费马猜想

辽宁教育出版社

名题欣赏

51
3

VISIT…

LANZAROTE Caliente.com



责任编辑：俞晓群
谭　坚
封面设计：安今生

ISBN 7-5382-0323-0/G·263
统一书号：7371·405
定　　价：1.70 元

世界数学名题欣赏丛书

费马猜想

姚玉强 编

辽宁教育出版社
1987年·沈阳

费 马 猜 想

姚玉强 编

辽宁教育出版社出版 辽宁省新华书店发行
(沈阳市南京街6段1里2号) 沈阳新华印刷厂印刷

字数:97,000 开本:787×1092 1/32 印张:7 插页:4
印数:1—4,000
1987年10月第1版 1987年10月第1次印刷

责任编辑:俞晓群 谭 坚 责任校对:理 广
封面设计:安今生

统一书号:7371·405 定价:1.70 元
ISBN 7-5382-0323-0/G·263

内 容 简 介

本书是“世界数学名题欣赏丛书”之一。书中较详细地介绍了费马猜想的历史和现状，包括历史上的主要成果以及解决问题的方法；一些近代成就；最后，对这个问题进行了有趣的推广。全书写法深入浅出，将知识性与趣味性融为一体，可供大、中学生及广大数学爱好者阅读。

Summary

This book is one of the world famous mathematics appreciation series. It systematically introduces the history of Fermat Guess and present condition, includes the main history achievements, ways of solving problems and some achievements in modern times. At last, it gives an interest popularization. The whole book explains the profound in simple terms, blends as well as knowledge and interest. It serves colledge students, middle school students and vast numbers of lovers of mathematics.

若无某种大胆放肆的猜想，一般是不可能有知识的进展的。

——高斯

序　言

什么是猜想呢？人们在数学研究中，经过大量的观察和实践，得到某种规律或结论，试图把它推广到一般，成为普遍的规律，这就是猜想或猜测。

在数学发展的历史长河中，数学家曾提出许多著名猜想。例如，“哥德巴赫猜想”、“费马猜想”和“四色猜想”等。它们象颗颗斑斓的明珠，闪烁着人类智慧的光芒。

希望并不一定是客观现实，猜想也不总是真理。欲想使猜想成为数学理论，还必须经过严格的逻辑证明。千百年来，数学家们继往开来，潜心思考，探求精蕴，取得了丰硕成果。有的猜想被证明是正确的，已经成为定理，也有的被证明是错误的。然而，至今仍有一些猜想向着人类的智慧挑战，人们不能肯定它是对的，也不能指出它是错误的，成为著名的数学难题。费马猜想就是其中之一。

费马猜想一经发表，引起许多著名数学家和广大数学爱好者的极大兴趣。内容之浅显似乎不难证明。然而，三百多年过去了，它仍然没有得

到最后解决。

现在费马猜想仍有巨大的吸引力。许多青少年数学爱好者跃跃欲试，希望摘取这颗明珠，为祖国赢得荣誉，为科学事业的发展做出贡献。

鉴于国内专门介绍费马猜想的书较少，笔者不揣学识浅陋，写了这本小册子。主要内容选自P·利奔波姆著《费马大定理十三讲》和B·夕宾斯基著《论方程的整数解》。本书比较系统地介绍费马猜想的历史与现状：一方面，介绍这个问题的基本内容和近代成果，另一方面，介绍一点解决问题的方法。考虑读者的数学基础，本书在编写上力求做到几下几点：

1. 放低起点，从基础知识谈起。研究费马猜想所涉及的一些基础知识，如整数论知识和代数数论知识，都做了简单扼要的介绍。还有的在注脚中加以说明。这样，具有中等数学知识的读者，只要逐步读下去，书中绝大部分内容都可以读懂。

2. 通俗易懂，深入浅出。叙述通俗，解释浅显：有的结果只介绍而未加证明；有的定理在证明中不涉及高深理论时，给出了证明，这些证明中包括了一些基本方法的运用。

3. 趣味性。介绍一些科学家的轶事和某些

结果的发现的趣闻。

本书试图使广大青少年读者知道，费马猜想的解决是十分艰难的，只有打好坚实的基础，才有可能攻克这个难题。读了本书后，如果能对费马猜想引起兴趣，在将来攀登时起着一层阶梯作用，这才是编者的期望。

本书的编写得到辽宁师范大学梁宗巨教授的热情指导。梁教授审查了初稿，在书的宗旨、取材、写法及科学家译名等方面都提出十分宝贵意见。这些使笔者受益匪浅，也给本书增添了特色。南开大学胡久稔副研究员也审阅了书稿，并提出了许多好的意见。在此，谨向他们致以诚挚的谢意。

由于编者学识水平所限，遗漏和错误在所难免，希望专家和读者指正。

姚玉强

1986年10月于沈阳

世界数学名题欣赏丛书

欧几里得第五公设
连续统假设
费马猜想
黎曼猜想
科克曼女生问题
斐波那契数列
希尔伯特第十问题
不动点定理
哥德尔不完全性定理
无处可微的连续函数
哥德巴赫猜想
货郎担问题
置换多项式及其应用
素数判定与大数分解

C1-51
1:3



作者简介

姚玉强，1937年11月生于辽宁省盖县。1960年毕业于辽宁大学数学系。现在沈阳市教育学院数学系任教。讲师，代数教研室主任。译著有《新符号问题与整数问题》（人民教育出版社）。

目 录

一 费马猜想的历史……………………………………1
（一）费马猜想的来源………………………… 4
（二）早期的尝试………………………………11
（三）库麦的贡献………………………………17
（四）金质奖章和十万马克奖金…………20
（五）费马曲线…………………………………24
（六）其他一些结果……………………………25
（七）近代成果…………………………………27
（八）费马猜想的意义…………………………33

二 早期成果的说明……………………………………39
（一）整数的基本性质…………………………42
（二）勾股方程…………………………………54
（三）无穷递降法………………………………61

（四）四次的费马方程……………………63
（五）三次的费马方程……………………67
1. 初等证明……………………………68
2. 欧拉的证明…………………………75
3. 高斯的证明…………………………78
（六）五次的费马方程……………………88
（七）七次的费马方程……………………89

三　朴素的方法………………………………93
（一）巴罗和阿贝尔的关系式……………95
（二）热尔曼的理论………………………97
（三）温特的定理…………………………101
（四）拾零…………………………………104

四　代数数论方法……………………………109

五　新近的成果………………………………119
（一）$p<125000$ 费马猜想成立…………121
（二）欧拉数和费马猜想…………………127
（三）莫德尔猜想…………………………129
（四）数理逻辑方法………………………133

六　估计………………………………………137

（一）初等估计 ……………………………140
（二）土厄、罗思、西格尔和贝克 ……144
（三）新方法的应用 ………………………149

七　费马猜想的推广 ………………………155
（一）$x^3+y^3+z^3=w^3$ ………………………157
（二）$x^3+y^3+z^3=n$ ………………………162
（三）三次的方程 …………………………165
（四）四次的方程 …………………………171
1. $\Sigma x_i^4=y^4$ ………………………………171
2. $x^4+y^4=z^4+t^4$ ………………………173
3. $\Sigma x_i^4=\Sigma y_i^4$ ………………………173
4. $\Sigma x_i^4=ky^2$ ………………………………174
5. $x^4+ky^4=z^2$ ……………………………176
（五）n 次的方程 …………………………179
1. $\Sigma x_i^j=y^j$ ………………………………179
2. $ax^m+by^n=cz^l$ ………………………180
3. $x^3\pm y^2=z^n$ ………………………………182

结束语 ……………………………………187

参考文献 …………………………………193
中外人名对照 ……………………………196

Contents

I The History of the Fermat's Conjecture ········· 1

(I) The Source of the Fermat's Conjecture ········· 4

(II) Early Attempts ········· 11

(III) Kummer's Monument ········· 17

(IV) The Golden Medal and the Prize of 100000 Mark ········· 20

(V) The Fermat's Curve ········· 24

(VI) Other Relevant Results ········· 25

(VII) Recent Results ········· 27

(VIII) Meanings of the Fermat's Conjecture ········· 33

II Explanations of Early Results ········· 39

(I) Basic Properties of Integers ········· 42

(II) The Pythagorean Equation ········· 54

(III) The Method of the Infinite

Descent ……………………………61
(Ⅳ) The Biquadratic Equation………63
(Ⅴ) The Cubic Equation ……………67
1. Elementary Proof…………………68
2. Euler's Proof………………………75
3. Gauss's Proof………………………78
(Ⅵ) The Quintic Equation……………88
(Ⅶ) Fermat's Equation of Degree Seven ……………………………89

III The Naïve Approach……………………93
(Ⅰ) The Relations of Barlow and Abel ……………………………95
(Ⅱ) Sophie Germain's Theory………97
(Ⅲ) Wendt's Theorem ………………101
(Ⅳ) Odds and Ends …………………104

IV The Method of Algebraic Number Theory……………………………109

V Fresh Efforts ……………………………119
(Ⅰ) Fermat's Last Theorem Is True for Every Prime Exponent Less Than 125000……121

(Ⅱ) Euler Numbers and Fermat's Conjecture……127
(Ⅲ) Mordell's Conjecture……129
(Ⅳ) The Logicians……133

VI Estimates……137
(Ⅰ) Elementary Estimates……140
(Ⅱ) Thue, Roth, Siegel and Baker……144
(Ⅲ) Applications of the New Method……149

VII Extensions of the Fermat's Conjecture……155
(Ⅰ) $x^3+y^3+z^3=w^3$……157
(Ⅱ) $x^3+y^3+z^3=n$……162
(Ⅲ) Equation with Three Exponent……165
(Ⅳ) Equation with Four Exponent……171
1. $\Sigma x_i^4=y^4$……171
2. $x^4+y^4=z^4+t^4$……173
3. $\Sigma x_i^4=\Sigma y_i^4$……173

4. $\Sigma x_i^4 = ky^2$ …… 174

5. $x^4 + ky^4 = z^2$ …… 176

(Ⅴ) Equation with n Exponent …… 179

1. $\Sigma x_i^j = y^j$ …… 179

2. $ax^m + by^n = cz^p$ …… 180

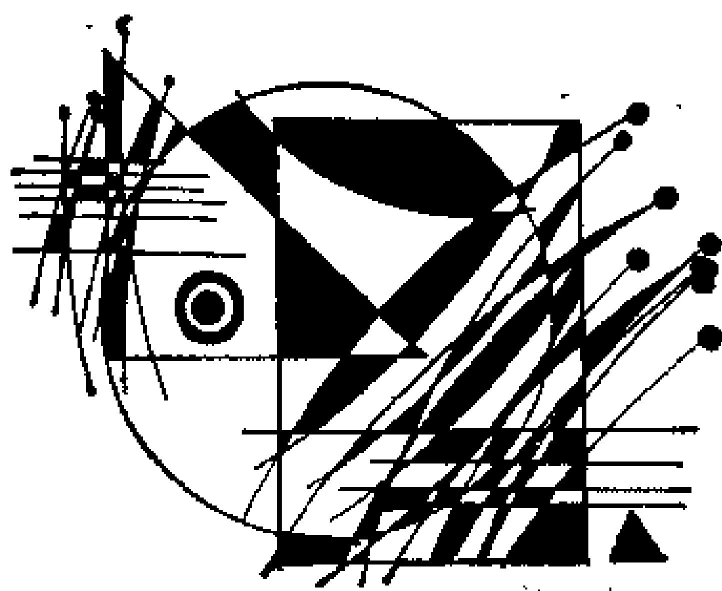
3. $x^2 + y^2 = z^n$ …… 182

Epilogue …… 187

Bibliography …… 193

Index of Names …… 196

一　费马猜想的历史



数论是数学的一门历史悠久的学科，不定方程又是数论中最古老的一个分支。所谓不定方程，简单地说，就是未知数的个数多于方程的个数。一般地，我们把不定方程（组）的解限制在整数、正整数或有理数的范围内。例如，求著名的勾股方程 $x^2+y^2=z^2$ 的整数解 x、y、z 就是不定方程求解问题。中国在研究不定方程上有着悠久的历史。在国外，古希腊数学家丢番图于公元三世纪初就研究过一些不定方程，并取得了很大成就。因而，对于整系数不定方程，如果只考虑它的整数解，则称为丢番图方程。

不定方程有着丰富的内容，与数学的一些分支如代数数论、代数几何、组合数论等有密切联系。古今中外许多优秀数学家对它进行过研究，这些研究大大丰富了数论的内容。但是，从

整个说来，不定方程还有着广阔的未知领域。因此，它仍然并将继续吸引着广大数学家的注意，这方面的研究正是方兴未艾。

这本小册子试图介绍这方面的部分内容，即著名的费马猜想及其有关知识。从这个侧面可以看到不定方程的丰富内容，以及它在数学发展中所起着的巨大推动作用。

本书以后把不定方程简称为方程。

（一）费马猜想的来源

什么是费马猜想呢？要说清这个问题，让我们简单地回忆一下它的历史。

费马是十七世纪最卓越的数学家之一，1601年8月20日出生在法国南部土鲁斯附近的博蒙—德洛马涅，父亲是一位皮革商，1665年1月12日逝世于土鲁斯或卡斯特。

费马在大学里专攻法律，学成后回到家乡城市土鲁斯做律师，以法律知识渊博，做事清廉而著称。他是土鲁斯议会议员，终身职业是律师，做了土鲁斯议会的三十年法律顾问。

费马是一位博览群书，见多识广的学者，又

是精通多种文字的语言学家。业余时间喜欢恬静生活，全部精力花费在钻研数学和物理问题上，有时用希腊文、拉丁文和西班牙文写诗作词，自我朗诵消遣。

虽然费马年近三十才认真注意数学，但他对数论、几何、分析和概率等学科都做过深入的研究，做出了重大的贡献。今天，他的名字几乎与数论是同义语，他给出素数的近代定义，并且提出一些重要命题；他又同笛卡儿分享着创立解析几何的荣誉；他被公认为数学分析的先驱之一；他和帕斯卡等同是概率论的开拓者。因此，费马被誉为“业余数学家之王”，与同时代的数学大师笛卡儿、莱布尼茨等齐名。

费马谦虚谨慎，鄙薄名利，生前很少发表著作，他的卓识远见出于他与同时代学者的信件和一批以手稿形式传播的论文。他的崇拜者常常催促他发表著述，但都遭到拒绝。他的很多论述，特别在数论方面的论述，从没有正式发表过。费马死后，很多论述遗留在故纸堆里，或阅读过的书的页边空白处，书写的年月无从查考；还有的保留在他给朋友们的书信中。他的儿子 S·费马将遗稿进行了整理，汇编成册，共分两卷，分别于1670年和1679年在土鲁斯出版。第一卷有丢番

图的《算术》，带有校订和注解；第二卷包括抛物形求面积法，极大极小及重心的论述，各类问题的解答，这些内容后来成为微积分的一部分。还有球切面，曲线求长等。另外，还有他和同时代的许多数学家和物理学家笛卡儿、帕斯卡和惠更斯等的通讯函件。费马猜想以这种方式公布于世。

人们对于方程

$$x^2+y^2=z^2$$

的整数解的研究要追溯到遥远的古代。长期以来，中外许多数学家各自做出了不同的贡献。

十七世纪初期，数学家开始寻找方程

$$x^3+y^3=z^3,\quad x^4+y^4=z^4$$

等的正整数解。

古希腊数学家丢番图著《算术》一书。1621年，数学家巴切将《算术》从希腊文译成拉丁文，在法国出版。费马买到了它，对于其中的数论问题产生浓厚的兴趣。公余之时，对希腊数学家的一些问题进行研究和推广。当他读到第Ⅱ卷第八命题"将一个平方数分为两个平方数"时，他想到了更一般的问题。于是，他在页边空白处用拉丁文写了如下一段话：

Cubum autem in duos cubos, aut

quadrato — quadratum in duos quadrato — quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

其意思是："将一个立方数分为两个立方数，一个四次幂分为两个四次幂，或者一般地将一个高于二次的幂分为两个同次的幂，这是不可能的。关于此，我确信已发现一种奇妙的证法，可惜这里的空白太小，写不下。"这段叙述用现代数学语言来说，就是

当整数 $n>2$时，方程

$$x^n+y^n=z^n \quad (1)$$

没有正整数解。

这就是费马猜想。

费马猜想(Fermatsche Vermutung)，又叫做费马问题(Fermatsches Problem)，但更多地叫做费马最后定理(Fermat's Last Theorem)，我们把它简记为 FLT．中国较普遍叫做费马大定理。

从费马研究丢番图的书到他逝世有三十年的

时间，在这种情况下，方程（1）的解的定理无疑不是他的最后定理。为什么这样叫呢？数学家们解释说，名字的来源很大可能是费马提出很多数论命题，后来的数学家经过长期努力，证明大部分是正确的，只有一个是错误的。到1840年左右，只剩下 FLT 没有被人证明，因此称为最后定理。

我国叫费马大定理，是为了区别费马小定理（参见第一部分（二））。

写着这段笔录的书丢失了，但在1670年由他儿子 S· 费马出版的费马著作中有此记载。迪克森的《数论史》第Ⅱ卷中说，费马的断言大约产生在1637年。理由是费马家的皮革厂（1883年）提到费马给梅森的信，信中写到，他希望找到两个立方数的和是一个立方数，两个四次幂的和是一个四次幂。这封信的日期是1638年6月。费马于1640年和1657年将同样内容推荐给一些数学家，但都没有提到他找到的奇妙的证明。

因为丢番图的《算术》仅论及有理数，所以费马的意思是不存在有理数 x、y、z 使（1）成立。如果x、y、z 可以取无理数，那么对于数对 x、y，得到 $z=\sqrt[n]{x^n+y^n}$，即容易证明FLT不成立。但是，如果（1）存在有理数解，那么

（1）存在整数解．这是清楚的，众所周知，如果有理数 x、y、z 适合方程（1），d 是它们分母的最小公倍数，那么 xd，yd，zd 都是整数，并且 $(xd)^n+(yd)^n=(x^n+y^n)d^n=(zd)^n$。因此，整数 zd的 n次幂是两个整数 xd 与yd的 n 次幂的和．此外，丢番图和费马都论及正数（在费马时期，负数和零仍被怀疑）。因此，x 或y 为零的情况不言而喻也被排除（例如，$2^5+0^5=2^5$自然与 FLT相违）．当（1）的解x,y,z中有零时，则称此解为平凡解．

现在，我们对方程（1）做一些讨论。

如果 $(x, y)=d$，那么 $d\mid z$。设 $x=dx_1$，$y=dy_1$，$z=dz_1$，则（1）可写成

$$(dx_1)^n+(dy_1)^n=(dz_1)^n$$

约去 d^n，得

$$x_1^n+y_1^n=z_1^n$$

其中x_1，y_1，z_1 是正整数，并且$(x_1, y_1)=(x_1, z_1)=(y_1, z_1)=1$．因此，在（1）中可假设 x，y，z 两两互素．（1）的两两互素解，称为原始解．

注　符号$(a, b)=d$，$(a, b)=1$，$a|b$ 的意义参见第二部分（一）．

如果对于正整数m定理成立，并且 $n=lm$，

其中 l 是正整数，那么对于 n 定理也成立。否则，如果 x，y，z 是非零整数，并且 $x^n+y^n=z^n$，那么 $(x^l)^m+(y^l)^m=(z^l)^m$，同假设矛盾。

设 n 是一个大于2的整数。当 n 为奇数时，n 一定能被一个奇素数整除。当 n 为偶数时，则 $n=2m$，其中 m 是正整数；若 m 是奇数，m必被一个奇素数整除，若m是偶数，则$n=2m$ 被4整除。由上述讨论可以得出结论：任何一个大于2的整数 n，或是4的倍数，或是一个奇素数的倍数。因此，证明FLT，实际上只需证明

$$x^4+y^4=z^4$$

和

$$x^p+y^p=z^p,\ p\ 是奇素数$$

都没有正整数解便可。前者无解是容易证明的，后者无解的证明却是异常困难的。

为了证明的方便，经常把 FLT 分为下列两种情形：

第一种情形　对于素指数p，不存在整数 x，y，z，使 $p\nmid xyz$，且 $x^p+y^p=z^p$。

第二种情形　对于素指数 p，不存在整数x，y，z，使 $p\mid xyz$，且 $x^p+y^p=z^p$。

三百多年过去了，费马猜想仍没有最后得到

解决，它难住了所有数学家，成为数学著名难题之一。

（二）早期的尝试

费马的遗著发表了，人们很想从中知道费马是怎样证明FLT的，但查遍了他所有的著作，结果使人们大失所望。关于他的“奇妙的证明”，人们有各种猜测：有人认为他根本没有给出证明；相反，有人却认为他给出过证明，不过证明中有错误。前者认为，长期实践证明，用费马时期的数学知识没法给出证明。后者的理由有四条：

从费马的品德和才智来说，他不会自我欺骗，并能给出证明，这是其一。

其二，费马在同本书上还写了几个研究结果，如

1．任何形如$4n+1$的素数可以唯一地表示成两个整数的平方和，而$4n-1$型素数则不能。

2．对于整数n和素数p，$p\nmid n$，那么n^p-n可以被p整除，即费马小定理。

3．$x^2+2=y^3$只有一个整数解$x=5, y=3$。

这些结论费马都没有写出证明，后来，数学家证明

它们都是正确的。

其三，费马自己证明了$n=4$情形的 FLT，使用的是他发现的“无穷递降法”。后来发现无穷递降法对一般情形不适用。从而得出结论：费马可能在这方面犯了错误，而误认为发现了“奇妙的证明”。

最后，在数论的历史上，就是大数学家也难免犯错误。正是“智者千虑，必有一失”。费马也不例外，他也曾有过错误的猜想。例如，形如

$$F_n=2^{2^n}+1,\ n=0,\ 1,\ 2,\cdots$$

的数叫费马数。1640年，费马验证了

$F_0=3$，$F_1=5$，$F_2=17$，$F_3=257$，$F_4=65537$
是素数后，就猜想：$n\geqslant 0$时，F_n都是素数。1732年欧拉证明

$$F_5=2^{2^5}+1=641\times 6700417$$

即$641\mid F_5$，从而否定了这个猜想。

总之，各种猜测虽说法不一，但共同点是一个，都认为费马没有给出 FLT 的证明。现在看来，论证这个历史悬案对我们并不重要，而我们的任务是如何解决 FLT。

科学家踏上了征服 FLT 的漫长且艰难的历程。

FLT开始并没有引起人们瞩目，在一些著名

数学家受挫后，才普遍引起人们的重视。许多知名数学家都研究过它，他们中有欧拉、勒让德、高斯、阿贝尔、狄利克雷、拉梅、柯西和库麦等，有的人为此献出毕生精力，早期的库麦和近代的范迪弗就是其中的两位。据说林德曼在1882年证明π是超越数后，也终身从事FLT的研究。

注 人们把不是代数数的数称为超越数。关于代数数的意义，参看第四部分。

数学家继往开来，不畏劳苦，奋勇攻坚，在解决FLT上取得了很大成绩，并且发现了一些新方法和新理论，数学家也从中得到了磨练和启迪。

费马给朋友卡卡维的信中说，他已用无穷递降法证明$n=4$情形。但信中没有给出证明的细节。

1676年，贝西在费马的少量提示下，也给出这个情形的证明，论文刊在他死后出版的《论直角三角形的数学性质》一书中。

所谓无穷递降法，粗略地解释如下，假设某一个方程$f(x, y, z)=0$有整数解a，b，c，并且$c>0$，方法正是求另外的整数解a'，b'，c'，使$0<c'<c$，多次重复这个过程，得到解a''，b''，c''，并且$0<c''<1$。这是不合理的。无穷递降法不是别的，只不过是自然数的良序原理。

注 良序原理也叫最小数原理，其内容为自然数列中任意一个非空子列必有最小数。

给出这种情形的证明还有莱布尼茨(1678年)和欧拉（1738年）。

$n=3$ 的情形，早在972年阿拉伯人胡坚迪已经知道，但他的证明有缺陷。1770年欧拉首先给出这个特例的证明，不过这个证明不很完全。他引进一种形如

$$a+b\sqrt{-3}\text{，}a\text{、}b\text{ 是整数}$$

的数。这种数与整数有许多相似性质。欧拉发挥巨大想象力和创造力，用类比的方法，他假定整数的一些性质对 $a+b\sqrt{-3}$ 型数也成立，由此推出 $n=3$时FLT成立。

问题就出在这个假设上。我们知道，在整数中素因数唯一分解定理成立，即任何大于1的整数，如果不计素因数的次序，有且只有一种方法分解成素因数的乘积。由此可以推出，当两个互素的整数的乘积是某一个数的 n 次幂时，只有当其中每一个整数都是 n 次幂才行。欧拉假定这个性质对于$a+b\sqrt{-3}$型数也成立，由此进行推理，做出他的证明。事实上，整数与$a+b\sqrt{-3}$型数虽有许多相同性质，但还有许多不同性质，这就是欧拉的假定不够慎重之处。但是，对于

$n=3$ 情形，只要作些修补，实质上欧拉还是证明了 FLT。

欧拉的方法对以后的研究有很大启发性。稍后一些时候，数学家们致力于证明的基础研究，得到了一些有益成果。

注 关于整数一些性质和定理，详见第二部分（一）。

高斯给出 $n=3$情形的另外一个证明。

十九世纪二十年代，许多法国和德国数学家试图证明 FLT。

1823年，七十一岁高龄的勒让德给出 $n=5$情形的证明。

1825年，年仅二十岁的狄利克雷宣读一篇论文，他试图证明 $n=5$ 情形。事实上，他的证明不完全，这一点被勒让德指出。后来，狄利克雷独立地完成了证明，论文于1828年发表。他使用的方法本质是推广了欧拉用来证明 $n=3$ 情形的方法。

1832年，狄利克雷解决了 $n=14$的情形。

高斯试图证明$n=7$ 时的断言，但他失败了。由于失败的苦涩，他在1816年给奥尔伯斯的信中说：“我的确认为，费马定理作为一个孤立的命题对我没有多少兴趣，因为可以容易地给出许多那样的命题，人们不能证明它们，也不能否定它

们。”

后来，重要的进步归功于拉梅，1839年他证明 $n=7$ 的情形。不久后，勒贝格简化了拉梅的证明，他聪明地使用了恒等式

$$(x+y+z)^7-(x^7+y^7+z^7)$$
$$=7(x+y)(x+z)(y+z)[(x^2+y^2+z^2$$
$$+xy+xz+yz)^2+xyz(x+y+z)]$$

法国女数学家热尔曼在小指数特殊情形的研究中，取得很大成绩，给出一个著名定理。

首先是巴罗，后来的阿贝尔指出，如果 $x^p+y^p=z^p$，其中 x，y，z 不为零，则 x，y，z 必须满足一些有趣的关系式（详见第三部分（一））。通过聪明地变换，热尔曼证明：

如果 p 是一个奇素数，使 $2p+1$ 也是一个素数，那么对于 p，FLT的第一种情形成立。

存在许多素数 p，使 $2p+1$ 也是素数。例如，$2\times2+1=5$，$2\times3+1=7$，$2\times5+1=11$ 等。但是，仍然不知道是否存在无穷多这样的素数。

按照热尔曼的思想，勒让德推广热尔曼的定理如下：

如果 p 是素数，使 $4p+1$，$8p+1$，$10p+1$，$14p+1$，$16p+1$ 之一也是素数，那么对于指数 p，FLT的第一种情形成立。

这个定理实际上证明了对于所有素指数 $p<100$，FLT 的第一种情形成立。

这里讲述一下热尔曼的身世是必要的．她的父亲是商人，母亲操劳家务，本人从没有进过任何专门学校，靠刻苦钻研，自学成才。

当时的学会规章不允许妇女出席会议。热尔曼把论文用信件通知勒让德和柯西。她的文章得到了肯定。

热尔曼的成就令人震惊，得到大数学家的称赞。德国哥廷根大学授予她荣誉博士学位。但遗憾的是，喜讯从柏林传到巴黎时，热尔曼早已与世长辞了。

（三）库麦的贡献

我们已经知道FLT 对于一些指数 n 成立。但是，对于任意的 n 还没有被证明。

德国数学家库麦继续了这项工作，他花了二十年的时间，获得了巨大的成功。他从神学转向数学，并做了高斯和狄利克雷的学生，后来在布勒斯劳和柏林做了教授．虽然库麦的主要工作是在数论方面，但他在几何学方面还做出了漂亮的发

现；在大气对光的反射研究中也做出贡献。

库麦把 x^p+y^p（p为素数）分解成

$$(x+y)(x+ay)\cdots(x+a^{p-1}y)$$

这里a 是一个p 次单位根，又是Q上 $p-1$ 次不可约多项式

$$x^{p-1}+x^{p-2}+\cdots+x+1$$

的根。

他引进形如

$$f(a)=a_0+a_1a+\cdots+a_{p-2}a^{p-2}$$

的数，其中 a_i，$i=0$，1，2，…，$p-2$ 是整数。库麦把数 $f(a)$ 叫做复整数。我们把 $f(a)$ 称为分圆整数（参见第四部分）。

1843年，库麦对复整数进行了研究，给出素整数、可除性以及类似的东西的适当定义，并假定在分圆整数中唯一因子分解成立，由此出发，他给出了FLT的一个"证明"。同年他把手稿寄给狄利克雷，狄利克雷看过后，指出他的假设对证明费马定理是必需的，但假设没有一般性，即唯一因子分解仅对某些素数p 成立。1844年库麦认识到狄利克雷批评的正确性，他证明分圆整数唯一因子分解定理不是普遍成立。

还有两位著名数学家也犯了与库麦同样的错误。一位是柯西，另一位是拉梅。后者在此问题

上处境十分尴尬。

事情经过是这样的：在法国科学院的一次会议上，拉梅宣布他利用分圆整数理论证明了FLT。可是，当他宣讲证明概要后，刘维尔马上站起来反对，指出拉梅把通常整数的性质用到分圆整数上是不妥的。然而，这篇错误的论文已经发表在法国科学院的报告上，传遍整个数学界。拉梅十分懊悔，他写给柏林的狄利克雷的信中说：“只要是你在巴黎或者我在柏林，这一切都不会发生。”

为了使唯一分解成立，库麦从1844年开始一系列的研究，创立理想数的理论。他利用理想数，成功地证明对于许多素数FLT是正确的。在前一百个自然数中，只有37，59，67不为库麦的证明所包括。为了摈除这三个例外，库麦在1857年的一篇论文中将他的结果扩展到这些例外素数。可惜还是有缺点。直到1892年，$p=37$的情形才被米里曼诺夫证明。

由于库麦这项开创性贡献，1857年法国科学院给他颁发价值三千法朗的金质奖章。

高斯的学生戴德金以全新而有启发性的方式探讨唯一分解问题。1871年戴德金在他所编辑的狄利克雷的《数论》一书附录中，推广了高斯的复整数和库麦的代数数理论，创立现代代数数理论。

克罗内克是库麦的得意门生，他接替库麦在柏林大学任教授，继续研究代数数问题，沿着类似于戴德金的路线发展了它。

代数数论的工作，在十九世纪以希尔伯特的论代数数的著名报告为顶峰。在这个报告里，希尔伯特重新理论了这个世纪里的早期理论，并且给出获得这些结果的新颖、漂亮和强有力的方法。

代数数论本来是研究FLT解的一种方案，而现在，自身却变成了一个目的。它的创立被认为十九世纪代数学上最大成就。

（四）金质奖章和十万马克奖金

1823年和1850年，法国科学院曾先后两次提供金质奖章和三千法朗奖金，奖励证明FLT的数学家。1856年的鉴定人有柯西、刘维尔、拉梅、伯传德和沙尔。

布鲁塞尔科学院也以重金悬赏。

1908年，德国达姆施塔特城的数学家佛尔夫斯克尔遗言，把十万马克的巨款赠给哥廷根皇家科学会，有一个附加条件，将款项作为奖金，授

予第一个证明FLT的人。按照哥廷根皇家科学会的决定，这种证明必须在一种杂志上或者作为单行本发表，该会不负鉴定稿件之责；得奖最早须在著作发表两年以后。这项奖金限期100年，到2007年取消。在奖金发出之前，所得利息用来奖励在数学上做出重大贡献的人。曾几次照条件规定发过奖，其中一次获奖人是外斐力什，他在一篇著作中对 FLT 的证明确有重大贡献（参见第一部分（六））。

十万马克的奖金推动了 FLT 的研究。消息传出后，在德国和世界各地掀起了一股研究FLT的热潮。早些时候，每个稍有时誉的数学家，尤其是数学杂志的编辑们，都忙于处理所谓“几何作图三大不能问题”解法探求。这时，它们被FLT的解答所代替。应征者不仅有数学家，还有许多工程师、牧师、教员、大中学校的学生、银行职员和政府官员等；不仅有德国人，还有大量外邦人。人数之多，阶层之广，都是空前的。

注 几何作图三大不能问题，是指化圆为方问题，任意角三等分问题和立方倍积问题。

应征者的“证明”纷纷传来，单就1908至1911三年间，就收到一千份证明。然而，毫无例外，所有应征者的方法和证明都是错误的。不但

数学爱好者犯有错误，而且著名的数学家也被指出疏忽和遗漏。

当时，德国有一种叫《数学和物理文件实录》的数学刊物，曾设立固定部门，自愿对这方面论文进行鉴定。到1911年初，该部门审查111篇论文，全部发现错误。审稿的沉重负担使它承受不了，被迫宣布停止这方面工作。

为了减轻审查稿件的沉重负担，当年主管这方面工作的部门规定，寄来的答案必须是印刷件。数学家兰道出了个主意，印制一份复函的标准格式，上面写道：

亲爱的先生（女士）：

您对费马大定理的证明已经收到，现予退回。第一个错误出现在第____页第____行，……

兰道将这些明信片分发给他的学生们，吩咐他们将相应的数字填上去。

在数以千计的“证明”中，难免有粗制滥造的情形。例如，有一个证明只寥寥几句话：

已知 $a^2+b^2=c^2$，现在又设

$a^n+b^n=c^n$，则必须是 $n=2$。

但这与题意不符，因此证明其不可能。

还有的证明被指出错误，经过二次、三次、……诸次补充修正，结果还是不正确。对于这种局面，数学家丹吉格遗憾地指出："我们非常赞许这些人的热情，但是，可惜得很，他们之中的大多数人对于前人的成果毫无所知，甚至连库麦那样创造性贡献也不了解。当然，并不是说，非要应用库麦的方法才行，不过，毕竟他已经替我们进行这方面的研究数十年。"

1918年11月第一次世界大战结束后，战败的德国经历了一段非常混乱时期，国内生活动荡不定。1922年新政府发行大量纸币来适应财政的需要，爆发了严重的通货膨胀，马克不断贬值。例如，一本《数学年鉴》，1920年的价格是64马克，到1922年初涨了一倍，同年底涨到400马克，1923年变成800马克，到该年底竟达28000马克。这时，十万马克的奖金其实际价值只能买几张白纸！解答 FLT 的热潮至此才算告一段落。那些为奖金而努力的人不再作尝试；继续注意这个问题的人，大都是从爱好数学的立场出发。因此可以说，此后的研究才向着满足知识及创造成绩两大方向迈进。英国数学家莫德尔深有感触地说："如果你想发财，任何种方法都比证明费马猜想容易得多。"

到2007年还有二十几个春秋，能否有人获得这笔奖金，人们在翘首以待。

（五）费马曲线

这里，我们从函数观点介绍方程 $x^n+y^n=z^n$ 的性质，给出 FLT 的几何直观说明，它将有助于了解最近在 FLT 上所取得的重大突破（参见第一部分（七））。

方程

$$x^n+y^n=z^n,\ n>2$$

两端同除以 z^n，变为

$$x^n+y^n=1 \qquad (1)$$

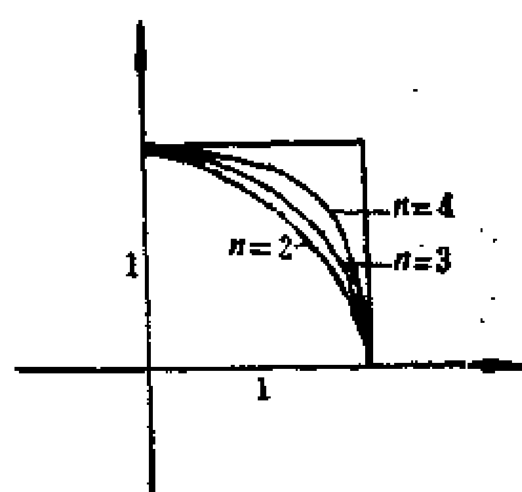
其中 x，y 为有理数。这时，FLT 等价于方程（1）没有非零的有理数解 x，y。

从（1）我们可以得到

$$y=\sqrt[n]{1-x^n} \qquad (2)$$

现在来研究函数（2）的几何意义。我们称函数（2）在 XOY 平面上的图象为费马曲线。当 $n=3$ 和 4 时，在第一象限内可以画出相应的费马曲线（如图）。当 n 增大时，费马曲线逐渐趋向与单位正方形相合。以这种现象解释 FLT，就

是：对于 $n>2$ 情形，费马曲线不通过 XOY 平面上坐标值是有理数的点，也就是说，无穷多费马曲线随处穿插于错综复杂分布的各有理点之间，但却无一处触及它们。这就是FLT制造出的一种奇观。



（六）其他一些结果

首先，让我们总结一下库麦以前在 FLT 上取得的主要结果。现列表如下：

指数	证明人	证明时间
$n=4$	费马	
	贝西	1676
	莱布尼茨	1678
	欧拉	1738
$n=3$	欧拉	1770
	高斯	

指数	证明人	证明时间
$n=5$	勒让德	1823
	狄利克雷	1825
$n=7$	拉梅	1839
$n<100$	库麦	1844—1857

热尔曼和勒让德证明素指数 $p<100$ 时，FLT的第一种情形成立。

其次，关于 FLT 的第一种情形还有两个较好结果。

本世纪初，关于第一种情形才出现突破性工作。1912年，福特翁勒证明下列两个定理：

定理1 如果p是奇素数，x，y，z是互素的整数，使 $x^p+y^p+z^p=0$，r 是自然数，使 $r\mid x$，$p\nmid x$，那么 $r^{p-1}\equiv 1 \pmod{p^2}$。

注 $a\equiv b \pmod{m}$ 是同余符号，意思是 $m\mid(a-b)$（详见第二部分（一））。

由此可得

推论（外斐力什，1909）方程

$$x^p+y^p+z^p=0,\quad p\nmid xyz$$

有整数解 x，y，z，则

$$2^{p-1}\equiv 1 \pmod{p^2}$$

最初确定在 $p<3700$ 的范围内只有1093，3511两个数使上列同余式成立；现在确定在 $p<$

31059000 的范围内也只有这两个数使同余式成立。

定理2 如果 p 是奇素数，x，y，z 是互素的整数，使 $x^p+y^p+z^p=0$，且 r 是自然数，使 $r\mid(x-y)$，$p\nmid(x^2-y^2)$，那么

$$r^{p-1}\equiv 1 \pmod{p^2}$$

推论 方程

$$x^p+y^p+z^p=0,\ p\nmid xyz,\ p>3$$

有整数解，则

$$3^{p-1}\equiv 1 \pmod{p^2}$$

1941年，D.H.雷麦和 E.雷麦证明

定理3 如果 FLT 第一种情形成立，那么

$$q^{p-1}\equiv 1 \pmod{p^2}$$

对于所有素数$q\leqslant 43$都成立。

利用这个结果，证明$p<253747887$时，FLT 第一种情形成立。

（七）近代成果

这里要介绍这样几个问题：

对于哪些指数 FLT 是真的；关于 FLT 的哪些工作还在进行；近几年的几项重大成果等。

目的是指出重大的历史发展。由于解决问题所需的各种方法，包括不同的技术，一般都要涉及高深的知识，这里只能简要地介绍结果。

首先，我们给出十个现代结果，其中某些结果在后面有关部分里还要作进一步说明。

1．瓦格斯塔夫（1977）：对于每一个素指数$p<125000$ FLT成立。

前不久，美国加利福尼亚大学伯克利分校的罗瑟教授，又把 p 的上限从12万5千推到4100万。

2．莫利斯玛等（1948）：对于每一个素指数 $p<57\times10^9$ FLT第一种情形成立（或者按照波利尔哈特等的结果，在最坏情况下，$p<3\times10^9$）。

事实上，对于更大的素指数 p第一种情形也成立。

3．对于现在已知的最大素数 FLT 第一种情形成立。目前已知的最大素数是梅森数$M_{86243}=2^{86243}-1$，这是1983年计算机专家斯洛文斯基在每秒运行一亿次的超巨型计算机 CRAY—1上运行5782秒得到的结果。

注 形状如2^n-1的数叫梅森数，记作$M_n=2^n-1$。

上面的结果是乐观方面。但是，一些数学家

考虑 FLT 可能存在反例。对于给定的指数 p，最小的反例有多大呢？

4．依恩柯利（1953），如果对于指数p第一种情形不成立，x，y，z 是整数，$0<x<y<z$，$p\nmid xyz$，$x^p+y^p=z^p$，那么

$$x>\left(\frac{2p^3+p}{\log(3p)}\right)^p$$

在第二种情形下，

$$x>p^{3p-4} \text{ 和 } y>\frac{1}{2}p^{3p-1}$$

此外，卡绍于1958年证明在第一种情形下，

$$y>\frac{1}{2}(p^3P+1)^p$$

其中P是所有这样的素数 $q\neq p$ 的积，$q-1$整除$p-1$。

费马方程也可能存在有限个解，这方面有：

5．依恩柯利和海罗（1964）：1）给定 p 和 $M>0$，至多存在有限组（x，y，z），使 $0<x<y<z$，$x^p+y^p=z^p$，且 $y-x$，$z-y<M$。2）给定p，至多存在有限组（x，y，z），使$0<x<y<z$，$x^p+y^p=z^p$，且 x 是某个素数的幂。

对于每一个这样的数组，我们有有效的控制（这是很重要的新的特性）：

$$x<y<\exp\exp\{[2^p(p-1)^{10(p-1)}]^{(p-1)/2}\}$$

注　e^x可表示为$\exp x$。

另一类结果，对于偶指数有如下定理：

6．特亚尼安（1977）：如果 x，y，z 是非零整数，p是任意奇素数，并且 $x^{2p}+y^{2p}=z^{2p}$，那么 $2p$整除 x或者 y。换句话说，对于每一个偶指数FLT第一种情形是真的。

FLT对于无穷多素指数成立的可能性问题。在这方面，我们有：

7．罗特凯也维奇（1965）：如果辛泽尔关于梅森数的猜想是真的，那么存在无穷多素数 p，关于 p，FLT 第一种情形成立（辛泽尔猜想：存在无穷多非平方梅森数）。

下面的结果与分圆域$Q(\zeta)$ 的类群有密切关系，这里ζ是1的 p次原根。

注　关于分圆域$Q(\zeta)$的知识，详见第四部分。

8．范迪弗（1929）：如果$Q(\zeta)$ 的类数第二个因数 h^+ 不是 p 的倍数，并且所有贝努利数 B_{2np}（$n=1$，2，…，$(p-3)/2$）的分子都不是 p^3 的倍数，那么对于指数 p，FLT成立。

注　关于贝努利数B_m的定义参见第四部分。

9．爱斯勒（1965）：如果对于 p 第一种情形不成立，那么$p^{[\sqrt{p}]-1}$整除 $Q(\zeta)$的类数第一

因数 h^*，并且 $Q(\zeta)$ 的理想类群的秩 p 大于 $\sqrt{p}-2$。

注 〔a〕表示不超过 a 的最大整数，参见第二部分（一）。

10．波鲁克内（1975）：如果对于指数 p 第一种情形不成立，那么 p 的非正规指数，$ii(p)=\#\{k=2,4,\cdots,p-3 \mid p$ 整除贝努利数 B_k 的分子$\}$满足

$$ii(p)>\sqrt{p}-2$$

其次，近几年取得的几项重大成果如下：

1．前些年美国数学家曼福得证明，如果 $x^n+y^n=z^n$ 有整数解，那么这样的解是"非常少的"。这个结果意味着 FLT 成立的可能性很大，它是目前关于 FLT 的最好结果之一。他的方法是这样的：如果 $x^n+y^n=z^n$ 有无穷多整数解 (x_m, y_m, z_m)，我们按照 z_m 由小到大的次序排列这个数组，那么就能找到一个常数 $a>0$ 和另一个常数 b，使 z_m 恒大于 10^{4am+b}，这是一个天文数字！由于这个成就，1974年曼福得获得国际数学界最高荣誉——菲尔兹金牌奖，当时他年仅37岁。

2．1922年英国数学家莫德尔提出一个猜想：如果 $F(x, y)$ 为有理系数多项式及代数曲线 $F(x, y)=0$ 的亏格 $\geqslant 2$，那么 $F(x,y)=0$ 只

有有限多个有理解。

3．1985年，用解析数论的方法，爱德列曼和海斯——布朗证明了存在无穷多个素数P，使得FLT的第一种情形成立。这无疑是FLT的研究中又一突破性工作。

1983年联邦德国29岁的数学家伐尔廷斯证明莫德尔的猜想是正确的。这个结果使一大批不定方程的求解问题得到解决，对于 FLT 也是一个重大突破。从这个结果，可以推出费马曲线$x^n+y^n=1$（$n\geqslant4$）上只有有限个有理点，也就是说，如果方程 $x^n+y^n=z^n$（$n\geqslant4$）有解，则至多有有限多个（参见第五部分（三））。

伐尔廷斯的巨大成就轰动了数学界。各国数学家普遍感到兴奋与惊奇，并给予高度的评价。一些数学家认为，这个进展不是每年都能碰得上的结果，是一件罕见的大事。至少就数论这个分支而言，可能已经解决了本世纪中最重要的问题。可以预言，伐尔廷斯将是第二十届国际数学家大会颁发的菲尔兹奖的获得者。

值得指出的是，伐尔廷斯在证明莫德尔猜想时，使用了沙伐尔维奇等所创造的一套深刻的代数几何工具。因此，我国著名解析数论学家王元指出，解析数论专家不懂代数的时代从此结束

了。从这方面来说，伐尔廷斯的工作使数论各方面的专家懂得了相互了解的重要性，这对于今后的数论研究工作将起到积极作用。

（八）费马猜想的意义

数学家希尔伯特认为，鉴别好的数学问题的一般准则有两条：

首先，问题应具有“清晰性和易懂性。因为清楚的、易于理解的问题吸引着人们的兴趣，而复杂的问题使人望而生畏。”

“其次，为着具有吸引力，应该是困难的，但却不应是完全不可解决而使我们白费气力。”

FLT就是这样一个好的数学问题。它形式简明，内容易懂，连中学生都可以理解，实践证明它又是十分困难的问题。

希尔伯特又说：“要想预先正确判断一个问题的价值是困难的，并且是常常不可能的；因为最终的判断取决于科学从该问题获得的收益。”是的，现在给出 FLT 的全面评价为时尚早，但就目前来说，已经可以看出它有着十分重大的意义。大体说来，它有着以下四个方面：

1. 理论方面

美国数学家爱德瓦德说："数学家经常漂游在还未解决的问题的汪洋大海之中，但是力图解决 FLT 在将来正如过去一样，必将给我们带来数学上的进展。" FLT 是举世公认的数学难题之一。三个多世纪来，数学家们用尽了现有的各种理论和方法，都没有获得最后成功，说明要解决 FLT 不仅要有既深又广的数学知识做基础，而且必须将现在的理论和方法用出新水平，或者创造新的理论和发现新的方法，象费马的"无穷递降法"和库麦的"理想数论"那样。数学家对后者抱着极大的热忱。

1900年，在巴黎召开的国际数学家代表大会上，希尔伯特做了一次震动数学界的讲演，他站在数学发展的前沿，高瞻远瞩地提出尚待解决的二十三个问题。这些问题的解决大都是相当困难的。他没有把 FLT 列入二十三个问题中，但他把它作为一个典型例子，说明这样一个非常特殊、似乎不十分重要的问题会对科学产生怎样令人鼓舞的影响。

这里有一个传闻，据说希尔伯特曾宣称他能证明 FLT，但他认为，在解决FLT 的过程中能

给数学发展创造许多新途径，一旦解决了这个难题，这些有益的副产品就得不到了，所以他避而不去解决它。他满怀深情地说："我应更加注意，不要杀掉这只经常为我们生出金蛋的母鸡。"希尔伯特能否证明 FLT 无从考查，但探索FLT的证明是"生出金蛋的母鸡"之说，从 FLT 的历史来看却颇有一些道理的。

2．应用方面

数学是一门基础科学。随着科学技术的进步，不仅在自然科学中数学的作用越来越大，就是在社会科学中也得到广泛的应用。在解决FLT的过程中，势必推动着数学的许多分支的发展，从而促进科学技术的进步、以及整个人类的文明。科学技术生产力和精神力量是无法从经济上计算价值的，故我们称它们为"无价之宝"。

3．国际影响方面

在 FLT 的研究上，许多国家的数学家都做出了贡献。如果哪个国家的数学家能在这个问题上取得重大突破，或者给予最后解决，无疑标志着这个国家至少在这个问题上处于领先地位，象陈景润在哥德巴赫猜想上证得（1＋2）一样，

为祖国赢得荣誉。

注 大偶数表为一个素数及一个不超过两个素数的乘积之和，简记为(1+2)。

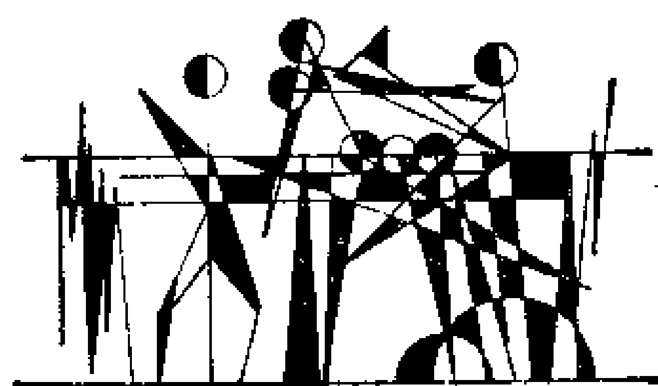
这里介绍一位数学家的轶事。本世纪著名的分析学家勒贝格创造了所谓"勒贝格积分理论"。这在分析学上是一个革命，大大推动了分析学的发展。勒贝格的晚年也沉醉于解决 FLT 中，他曾向法国科学院递交一份专论，叙述用他的理论可以彻底解决 FLT。法国科学院接着这个报告后，科学家们欢欣鼓舞，由于勒贝格的声望，科学家对他的理论抱着极大的希望。如果他的理论成立，三百多年中最难的数学问题之一，由法国人提出，最终又被法国人解决，以此可以说明法国人的聪明才智，值得向全世界骄傲。后来，一大批数学家研究了勒贝格的手稿后，非常扫兴地宣布，他也犯了错误，因此还是不成功。勒贝格接到退稿时，喃喃自语："我想，我这个错误是可以改正的。"可是，直到他逝世时还没有改正过来。

4. 批判唯心主义方面

国际上有人散布唯心主义的不可知论，其主要论据之一是FLT。他认为，FLT 从内容上说来

是很简单的，但人们研究了三百多年却解答不了。由此看来，人类虽然比其它动物聪明得多，但也不是无所不能的，人类的思维能力有个限度，而现在仿佛看出这个限度了。很明显，这是利用 FLT 宣扬唯心主义。可见，如果能完全解决 FLT，对于捍卫唯物主义，批判唯心主义，也是十分有益的。

二　早期成果的说明



第一部分里，我们简单地介绍了在 FLT 上所取得的各种成果。这部分里，我们将对这些成果给予说明；这里着重说明库麦以前的早期成果，近代一些结论将放在以后几部分里介绍。具体说来是这样的：

首先，我们研究勾股方程，即$x^2+y^2=z^2$，这是由于它与费马方程$x^n+y^n=z^n$有着密切联系，介绍 $n=4$情形的证明时，要用到它的有关知识。

其次，我们将给出一些小指数的证明。

我们已经给出 FLT 的一些早期历史，现在的介绍将限制在技术细节上。

库麦以前考虑的所有方法，有着共同的朴素思想，通常它们仅应用有理数的性质。因此它们是初等的，但不缺乏灵巧性。相反，它们通常是很有用的手段。

（一）整数的基本性质

这里介绍整数的一些基本知识，包括整除性，素因数分解和同余等。

1．整数的整除性

我们把 1,2,3,…，n，…叫做正整数，又叫自然数；把 −1，−2，−3，…，$-n$，…叫做负整数；把正整数、负整数和零统称做整数。

显然，两个整数的和、差、积仍为整数，但两个整数相除（除数不为零），所得的商却不一定是整数。因此，许多整数问题都与整数除法有关，研究这些问题，就是整数的整除性。

我们用〔α〕表示不超过 α 的最大整数。例如，〔−2.5〕= −3，〔3.4〕=3,〔4〕=4，〔π〕=3。

关于〔α〕，显然下面不等式成立：

$$[\alpha]\leqslant\alpha<[\alpha]+1 \qquad (1)$$

现在取 α为有理数$\frac{a}{b}$ (a,b为整数，$b>0$)，则由（1）可以得到

$$0 \leqslant \frac{a}{b} - \left[\frac{a}{b}\right] < 1$$

或

$$0 \leqslant a - b\left[\frac{a}{b}\right] < b$$

由此可得

$$a = \left[\frac{a}{b}\right]b + r,\quad 0 \leqslant r < b \tag{2}$$

因此，我们得到下面的定理：

定理1 （带余数除法）任给两个整数 a，$b>0$，必存在两个整数 q 及 r，使得

$$a = qb + r,\quad 0 \leqslant r < b \tag{3}$$

并且 q 及 r 是唯一的。

证明 （2）已经指明存在性。我们只要证明唯一性就够了。

若还存在整数 q_1 及 r_1，使得

$$a = q_1 b + r_1,\quad 0 \leqslant r_1 < b \tag{4}$$

则从（3）和（4）可得

$$b(q - q_1) = r - r_1$$

即有

$$b|q - q_1| = |r - r_1|$$

因为 r 及 r_1 为小于 b 的正数，所以 $|r - r_1| < b$。若 $q \neq q_1$，则有 $|r - r_1| \geqslant b$，得出矛盾。故

有$q=q_1$，从而推出 $r=r_1$。□

（3）中的 q叫做不完全商，r 叫做余数。

当$r=0$时，（3）变成

$$a=qb \tag{5}$$

这时，我们就说 b整除 a，或a 被b整除，b是 a 的因数，a 是 b的倍数。我们用 $b|a$ 表示 b 整除 a，用$b\nmid a$表示 b 不整除 a。

现在我们给出整除的一些简单性质。

1） 若 $a|b$，$b|c$，则$a|c$。

证明 因为 $a|b$，$b|c$，故有整数 q_1，q_2 使 $b=q_2a$，$c=q_2b$。因此，$c=(q_1q_2)a$。由于q_1q_2是整数，所以 $a|c$。□

2）若 $a|b$，则 $a|bc$，c 是任意整数。

证明 因为 $a|b$，则有整数q 使 $b=qa$，因此，$bc=(qc)a$。由于 qc 是整数，所以 $a|bc$。□

3）若 $a|b$，$a|c$，则 $a|(b\pm c)$。

证明 因为 $a|b$，$a|c$，则有整数 q_1,q_2 使 $b=q_1a$，$c=q_2a$。因此，$b\pm c=(q_1\pm q_2)a$。又 $(q_1\pm q_2)$ 是整数，所以 $a|(b\pm c)$。□

由2）、3）及数学归纳法，立得

4）若 $a|b_i$，$i=1,2,\cdots,n$，则$a|(k_1b_1+k_2b_2+\cdots+k_nb_n)$，$k_i$，$i=1,2,\cdots,n$ 是任意整

数。

由4）可推出

5）若在一个等式中，除某项外其余各项都是 a 的倍数，则此项也是 a 的倍数。

6）若 $a|b$，$b|a$，则 $b=\pm a$。

证明 令 a,b 都不为零。因为$a|b$，$b|a$，则有整数 q_1,q_2 使 $b=aq_1$，$a=bq_2$。因此 $a=aq_1q_2$。约去 a 得 $1=q_1q_2$。整数 q_1,q_2 的积为1，故此两个整数必都为±1，因而，$b=\pm a$。□

现在我们讨论两个整数的因数与倍数问题。

设 a,b 是两个数，若 d 是 a 的因数，也是 b 的因数，则 d 叫做 a,b 的一个公因数。a、b 所有公因数中最大的一个叫做 a、b 的最大公因数，记作(a,b)。特别，若 $(a,b)=1$，则称 a,b 互素。

不难看出，a、b 的公因数与$|a|$、$|b|$的公因数相同，因而有

$$(a,b)=(|a|,|b|)$$

因此，我们讨论最大公因数，不妨就非负整数去讨论。

现在介绍一个求最大公因数的方法——辗转相除法。这个方法不但可以用来求两个正整数的

最大公因数，而且还可以借此推出最大公因数的一些重要性质。

设a,b是任意两个正整数。由带余数除法，我们可以得到下列等式：

$$a=bq_1+r_1,\quad 0<r_1<b$$
$$b=r_1q_2+r_2,\quad 0<r_2<r_1$$
$$\cdots\cdots\cdots \qquad (6)$$
$$r_{n-2}=r_{n-1}q_n+r_n,\quad 0<r_n<r_{n-1}$$
$$r_{n-1}=r_nq_{n+1}+r_{n+1},\quad r_{n+1}=0$$

因为每进行一次带余数除法，余数至少减1，而b是有限的，所以我们最多进行b次带余数除法，可以得到一个余数为零的等式，即$r_{n+1}=0$。上面的计算方法，叫做辗转相除法。这个方法是我国古代数学家首先创造的，在古算书里叫求一术。但在国外叫欧几里得除法。

定理2 若a,b,c是三个不全为零的整数，且

$$a=bq+c$$

则$(a,b)=(b,c)$。

由整除性质5）及最大公因数的定义，这个定理是不难证明的。

现在我们证明

定理3 设a,b是任意两个正整数，则

$$(a,b)=r_n$$

证明 利用（5）及定理2可以得到

$$r_n=(0,r_n)=(r_{n+1},r_n)=(r_n,r_{n-1})$$
$$=\cdots=(r_1,b)=(a,b)。\square$$

定理3给出一个求最大公因数的实际方法：当 a,b 中有一个为零时，(a,b) 等于不为零那个数；当 a,b 都不为零，$(a,b)=r_n$。

推论 若 $(a,b)=d$，则存在两个整数 s,t，使

$$as+bt=d$$

下面给出最大公因数的两个重要性质：

设 a,b 是两个正整数，则

1）$(am,bm)=(a,b)m$，这里 m 为任意正整数。

2）若 d 是 a,b 的任一公因数，则

$$\left(\frac{a}{d},\ \frac{b}{d}\right)=\frac{(a,b)}{d}$$

特别有

$$\left(\frac{a}{(a,b)},\ \frac{b}{(a,b)}\right)=1$$

证明 由（6）及定理2不难证明1）。利用1）的结果立即推出2）。$\square$

现在给出互素的两个性质：

1）若 $(a,b)=1$，$a|bc$，则 $a|c$。

证明 因为$(a,b)=1$，由推论可知，存在整数 s,t，使

$$as+bt=1$$

从而

$$acs+bct=c \tag{7}$$

由题设 $a|bc$，故 a 整除（7）的左端每一项，因此 $a|c$。□

2）若 b 与 a_1，a_2，…，a_n 都互素，则 b 与 $a_1a_2\cdots a_n$ 互素。

证明 由题设及推论，对于 a_i、b 存在整数 s_i、t_i，使

$$bs_i+a_it_i=1,\quad i=1,2,\cdots,n$$

把所有这 n 个式子乘起来，右边得 1， 左边有 2^n 项，其中有一项包含 $a_1a_2\cdots a_n$，而其余各项都包含 b。所以乘起来的式子可写成

$$bs+a_1a_2\cdots a_nT=1$$

由此可见，b 和 $a_1a_2\cdots a_n$ 任何公因式必整除 1，故两者互素。□

下面研究最小公倍数。

设 a,b,m 是正整数。若 $a|m$，$b|m$，则称 m 是 a,b 的一个公倍数。a,b 所有公倍数中最小的一个叫做 a,b 的最小公倍数，记作$[a,b]$。

关于两个数的最大公因数与最小公倍数的关系有下面的定理

定理 4 $[a,b]=\dfrac{ab}{(a,b)}$.

特别地，若 $(a,b)=1$，则 $[a,b]=ab$。

（证明略）

最大公因数及最小公倍数的概念可以推广到多于两个数的情形。

2. 素数 算术基本定理

定义 一个大于1的整数，如果它的正因数只有1及它本身，就叫做素数（或质数）；否则叫做合数。

以后我们用 p，p_1，p_2，… 表示素数。

由定义可以把自然数分为三类：1、素数和合数。

定理 5 设 p 为素数，a 是任一整数，则或 $(p,a)=1$，或 $p|a$。

证明 因为$(p,a)|p$，由素数定义，或$(p,a)=1$，或 $(p,a)=p$，即 $p|a$。□

定理 6 设 $a_1,a_2,\cdots,a_n$ 是 n 个整数，p 是素数。若 $p|a_1a_2\cdots a_n$，则p至少整除$a_1,a_2,\cdots,a_n$ 中的一个。

证明 若 $p\nmid a_i$, $i=1,2,\cdots,n$, 由定理5知 $(p,a_i)=1$. 再由互素性质2)得 $(p,a_1a_2\cdots a_n)=1$,与题设矛盾。□

定理7 (算术基本定理)任一大于1的整数 n,恰有一种方法分解成素因数的乘积。

证明 要证 $n>1$ 必能分解成下面的形式

$$n=p_1p_2\cdots p_s,\quad p_1\leqslant p_2\leqslant\cdots\leqslant p_s \tag{8}$$

其中 $p_1,p_2,\cdots,p_s$ 为素数,称为素因数,并且这种表示式是唯一的。

首先证明 n 一定能分解成(8)的形式。若 n 为素数,则(8)显然成立。若 n 为非素数,则必有

$$n=p_1n_1,\quad 1<p_1<n_1$$

这里素数 p_1 为 n 的最小正因数。若 n_1 为素数,则(8)已证;若 n_1 为非素数,则有

$$n=p_1p_2n_2,\quad 1<n_2<n_1<n$$

这里素数 p_2 为 n_1 的最小正因数。继续下去,可以得到$n>n_1>n_2>\cdots>1$. 这种过程最多不能超过 n次,故最后得

$$n=p_1p_2\cdots p_s,\quad p_1<p_2<\cdots<p_s$$

其中 $p_1,p_2,\cdots,p_s$ 为素数。

其次证明(8)的表示法是唯一的。若 n还可以分解成

$$n=q_1q_2\cdots q_t,\ q_1<q_2<\cdots<q_t \quad (9)$$

其中 $q_1,q_2,\cdots,q_t$ 为素数，由（8）和（9）得到

$$p_1p_2\cdots p_s=q_1q_2\cdots q_t \quad (10)$$

由定理6，存在 $p_k(1\leqslant k\leqslant s)$及 $q_l(1\leqslant l\leqslant r)$ 使

$$q_1 | p_k,\ p_1 | q_l$$

但 p_k,q_l 为素数，所以 $p_k=q_1,q_l=p_1$。又$p_1\leqslant p_k$，$q_1\leqslant q_l$，故 $q_l=p_1\leqslant p_k=q_1$，即 $p_1=q_1$。因此，从（10）得

$$p_2p_3\cdots p_s=q_2q_3\cdots q_t$$

同样可得 $p_2=q_2$。依此类推，最后得到$s=r$，且 $p_i=q_i$ $(1\leqslant i\leqslant s)$。唯一性得证。□

推论 任一整数 $n(n>1)$能够唯一地分解成

$$n=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s} \quad (11)$$

其中 $p_1,p_2,\cdots,p_s$ 是素数，$r_1,r_2,\cdots,r_s$ 是正整数。（11）叫做 n的标准分解式。

定理8 （欧几里得） 素数无穷多。

证明 我们用反证法。若素数只有有限个，设为 $p_1,p_2,\cdots,p_n$。令

$$N=p_1p_2\cdots p_n+1$$

则 $N>1$，并且 $p_1,p_2,\cdots,p_n$ 都不能整除 N，故 N 无素因数，这是不可能的。□

3．同余

定义 给定一个正整数 m，把它叫做模．如果用 m去除任意两个整数 a与 b 所得的余数相同，则我们就说a,b对模 m的同余，记作$a\equiv b\pmod{m}$．否则，我们说a,b 对 模m 不同余，记作 $a\not\equiv b\pmod{m}$．

定理 整数 a,b对模 m 同余的充分与必要条件是$m|a-b$，即$a=b+mt$，t是整数．

证明 设 $a=mq_1+r_1$，$b=mq_2+r_2$，$0\leqslant r_1<m$，$0\leqslant r_2<m$．若 $a\equiv b\pmod{m}$，则$r_1=r_2$，因此 $a-b=m(q_1-q_2)$．反之，若$m|a-b$，则 $m|[m(q_1-q_2)+(r_1-r_2)]$，因此 $m|r_1-r_2$．但 $|r_1-r_2|<m$，故 $r_1=r_2$．□

有了同余的概念，我们就可把余数相同的数放在一起，从而产生了所谓剩余类概念．对模m，用它去除任何整数所得余数 r，总满足$0\leqslant r\leqslant m-1$．若把余数为 r 的数放在一起，记作K_r，则可以把全体整数分为m个集合：$K_0,K_1,\cdots,K_{m-1}$，称它们为模m的剩余类．

剩余类具有下列性质：

1）每一个整数必包含在而且仅在上述一个集合里．

2）两个整数同在一个集合里的充分与必要条件是这两个整数对模m同余。

定义 若 $a_0, a_1, \cdots, a_{m-1}$ 是 m 个整数，并且其中任何两数都不在同一个剩余类里，则称a_0，$a_1, \cdots, a_{m-1}$ 为模 m的一个完全剩余系。

例如，$0, 1, 2, \cdots, m-1$ 便是模 m 的一个完全剩余系。

定义 我们把完全剩余系中与模m互素的整数全体叫做模m的一个简化剩余系。

例如，$m=10$时，1，3，7，9组成一个简化剩余系。

定义 欧拉函数 $\phi(x)$ 是定义在正整数上的函数，它在正整数 a上的值等于序列 $0, 1, 2, \cdots, a-1$ 中与 a互素的数的个数。

例如，$\phi(10)=4$，$\phi(5)=4$。

4．同余式

若 $f(x)$表示多项式 $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$，其中 a_n，a_{n-1}，$\cdots$，a_0 是整数，m 是一个正整数，则

$$f(x) \equiv 0 \pmod{m} \qquad (12)$$

叫做模m的同余式。若 $m \nmid a_n$ $\not\equiv 0 \pmod{m}$，则(12)叫做n次同余式。

若 a 是使 $f(a)\equiv0 \pmod m$ 成立的一个整数，则 $x\equiv a \pmod m$ 叫做同余式（12）的一个解。

（二）勾股方程

如果 x,y,z 分别表示直角三角形的两个直角边和斜边的长，则有

$$x^2+y^2=z^2 \qquad (1)$$

这就是著名的勾股定理。我们把方程（1）叫做勾股数方程。

如果正整数 x,y,z 适合方程（1），那么把它们叫做勾股数，或无零勾股数。如果勾股数 x,y,z 两两互素，那么称它们为基本勾股数。

求方程（1）的所有整数解，只须求出基本勾股数就足够了。所有另外的解，用改变符号，交换 x,y 和以某些非零的整数乘可以得到。

在寻找勾股数方面，我国有着悠久且光辉的历史。古算书《周髀算经》中，记述着公元前1100年周公和商高两个人的对话，商高说："句广三，股修四，径隅五。……"即给出了一组勾股数3，4，5。公元一、二世纪间的《九章算

术》中，记载的勾股数竟有八组之多，它们是：(3，4，5)，(5，12，13)，(7，24，25)，(8，15，17)，(20，21，29)，(20，99，101)，(48，55，73)，(60，91，109)。更有重大意义的是，近几年对《九章算术》进一步研究，数学史家指出，书中实际上给出了求勾股数的通式，即对于任意的正整数m,n，$m>n$，有

$$\begin{cases} x=m^2-n^2 \\ y=2mn \\ z=m^2+n^2 \end{cases}$$

并且刘徽给出了证明。这是第一个勾股方程解的通式。

公元前五、六世纪，古希腊数学家毕达哥拉斯在研究勾股定理方面做出了很大贡献，因而，国外把勾股定理叫做毕达哥拉斯定理，把勾股数叫做毕达哥拉斯数。

现在介绍（1）的解的通式。

我们讨论（1）的解的性质。

由于方程（1）是二次齐次式，故求（1）的非零整数解，只须求正整数解即可。因而，可假设 $x>0$，$y>0$，$z>0$。

如果（1）有正整数解 x,y,z，且 $(x,y)=d>1$，那么 $d^2|(x^2+y^2)$，即 $d^2|z^2$，而$d|z$，此时，

可从（1）的两端约去 d. 因而，可假定 $(x,y)=1$.

如果（1）有正整数解 x,y,z，且 $(x,y)=1$，那么 x,y 奇偶性相反。因为 $(x,y)=1$，显然 x,y 不能同为偶数。x,y 也不能同为奇数。否则，$x^2+y^2\equiv 2 \pmod 4$，$z^2\equiv 0$ 或 $1 \pmod 4$，显然（1）不成立。故可设 y 为偶数。

综上所述，欲求（1）的全部非零整数解，只须求满足上述三个假定的整数解就可以了。

定理1 方程

$$x^2+y^2=z^2 \tag{1}$$

满足条件

$$x>0,\ y>0,\ z>0,\ (x,y)=1,\ 2\mid y \tag{2}$$

的全部整数解可以由下列公式给出：

$$\begin{cases} x=u^2-v^2 \\ y=2uv \\ z=u^2+v^2 \end{cases} \tag{3}$$

这里

$$u>v>0,\ (u,v)=1,\ u,v \text{ 奇偶性相反。} \tag{4}$$

首先，我们证明两个引理。

引理1 如果 x,y,z 是方程（1）的解，并且满足条件（2），那么 $\frac{1}{2}(z+x)$，$\frac{1}{2}(z-x)$

都是整数，并且$\left(\frac{1}{2}(z+x), \frac{1}{2}(z-x)\right)=1$。

证明 由于 $2|y$，$(x,y)=1$，则x 为奇数。因而 x^2 为奇数，y^2 为偶数。由于 $x^2+y^2=z^2$，则 z^2 为奇数，从而 z 为奇数。因此，$z+x$，$z-x$ 都是偶数，故 $\frac{1}{2}(z+x)$，$\frac{1}{2}(z-x)$ 都是整数。假设$\left(\frac{1}{2}(z+x), \frac{1}{2}(z-x)\right)=d$，则

$$\begin{cases} \frac{1}{2}(z+x)=k_1d \\ \frac{1}{2}(z-x)=k_2d \end{cases}$$

其中 $(k_1,k_2)=1$。由此得 $x=(k_1-k_2)d$，$d|x$。又由（1）得

$$y^2=z^2-x^2=(z+x)(z-x)=4k_1k_2d^2$$

因而 $d^2|y^2$，$d|y$，故 $d|(x,y)$。但 $(x,y)=1$，所以 $d=1$。因此$\left(\frac{1}{2}(z+x), \frac{1}{2}(z-x)\right)=1$。□

引理 2 方程

$$uv=w^2 \tag{5}$$

满足条件

$$u>0,\ v>0,\ w>0,\ (u,v)=1 \tag{6}$$

的全部整数解可以写成

$$u=a^2,\ v=b^2,\ w=ab \tag{7}$$

其中

$$a>0,\ b>0,\ (a,b)=1 \qquad (8)$$

证明 设 u,v,w 是（5）的一组整数解，且满足条件（6）。令 $u=a^2u_1$，$v=b^2v_1$，a,b，u_1,v_1 都是正整数，且 u_1 和 v_1 不再有平方因子，则 $a^2|w^2$，$b^2|w^2$，进而 $a|w$，$b|w$。由于 $(u,v)=1$，则 $(a^2,b^2)=1$，进而 $(a,b)=1$。因此 $ab|w$。设 $w=abw_1$，代入（5），得

$$u_1v_1=w_1^2 \qquad (9)$$

如果 $w_1^2\neq 1$，那么存在素数 p，使 $p^2|w_1^2$。由于 u_1和v_1 的定义及 $(u_1,v_1)=1$，可知 $p^2\nmid u_1v_1$，与（9）矛盾。因此$w_1^2=1$，得 $u_1v_1=1$。但 w_1，u_1,v_1 都是正整数，故 $w_1=u_1=v_1=1$。因此，

$$u=a^2,\ v=b^2,\ w=ab$$

$$a>0,\ b>0,\ (a,b)=1$$

反之，满足（8）的（7）中的 u,v,w 显然适合（5），并且满足（6）。□

定理的证明 把（1）改写成

$$y^2=(z+x)(z-x)$$

或

$$\left(\frac{y}{2}\right)^2=\frac{z+x}{2}\cdot\frac{z-x}{2}$$

由引理1，$\frac{1}{2}(z+x)$ 和 $\frac{1}{2}(z-x)$ 都是整数，

并且$\left(\frac{1}{2}(z+x), \frac{1}{2}(z-x)\right)=1$。又由 $2|y$ 和引理2，则

$$\begin{cases}\frac{1}{2}(z+x)=u^2\\ \frac{1}{2}(z-x)=v^2\\ \frac{1}{2}y=uv\end{cases}$$

解得

$$\begin{cases}x=u^2-v^2\\ y=2uv\\ z=u^2+v^2\end{cases}$$

这里 $u>v>0$，$(u,v)=1$。因为 z 是奇数，$z=u^2+v^2$，所以 u,v奇偶性相反。

直接代入可验证，（3）式适合（1），

$$x^2+y^2=(u^2-v^2)^2+4u^2v^2=(u^2+v^2)^2=z^2$$

由于 $u>v>0$，所以 $x=u^2-v^2>0$，$y=2uv>0$，$z=u^2+v^2>0$，并且 $2|y$。设$(x,y)=d$，则 $d|z$，$d|(u^2+v^2)$，$d|(u^2-v^2)$，故 $d|2(u^2,v^2)$。但$(u,v)=1$，则 $(u^2,v^2)=1$，故 $d=1$ 或 2。因为x是奇数，$d|x$，所以$d=1$。因此，满足条件（4）的（3）中的 x,y,z 是（1）的解，并且满足条件（2）。□

这里还要指出，古代各国学者都没有考虑（1）的通解问题，研究这方面的问题是近代的事，上个世纪八十年代才求得（1）的整数解的通式。

由公式（3），从不同的数对(u,v)得到不同的基本勾股数。例如，最小的几组基本勾股数，依z值从小到大的顺序如下：

（3，4，5），（5，12，13），（15，8，17），（7，24，25），（21，20，29），（35，12，37），……

基本勾股数的列举相当于奇正整数分为两个整数平方和的表示法。关于这一点，费马证明熟知的定理：

定理2 如果 n 是正整数，$n=r^2n'$，并且 n' 不含平方因数，那么 n 能够表为两个平方数和的充分且必要条件是 n' 没有形如$4m-1$的素因数，其中 r,m是正整数。

然后，余下的问题是求一个整数表为两个平方数和的个数。

令 $r(n)$表示 $n=a^2+b^2$ 的整数对 (a,b)的个数，其中 a,b 不必为正数。例如 $r(1)=4$，$r(5)=8$，即$1=(\pm1)^2+0^2=0^2+(\pm1)^2$，$5=(\pm1)^2+(\pm2)^2=(\pm2)^2+(\pm1)^2$。

雅可比和高斯各自独立地求出 $r(n)$:

定理 3　$r(n)=4(d_1(n)-d_3(n))$

其中

$$d_1(n)=\#\{d\mid d\geqslant 1, d\mid n, d\equiv 1 \pmod 4\}$$

$$d_3(n)=\#\{d\mid d\geqslant 1, d\mid n, d\equiv 3 \pmod 4\}$$

定理 3 是说，$n=a^2+b^2$ 解的个数等于四倍于 n 的因数 $\equiv 1 \pmod 4$ 的个数减去 n 的因数 $\equiv 3 \pmod 4$ 的个数。

由于这个公式，确定所有的基本勾股数是可能的（对于确定的 z）。定理 3 的证明可在华罗庚的《数论导引》中找到。

（三）无穷递降法

费马发现了无穷递降法，他为此感到非常自豪。在他晚年的一封长信中，概括了他在数论中的发现，他明确地阐明，他的全部证明使用了这个方法。简单地说，方法是证明对于被证明的整数若干性质或关系是不可能的，如果它们对某些数成立，它们将对一些较小的数也成立；然后，用同样的论证，它们对一些更小的数也成立，无限地进行下去，这是不可能的，因为正整数序列

不能无限地减小。

这个方法是非常巧妙的，在研究不定方程问题上，是十分有用的。特别，在 FLT 的早期研究中，不止一次地用过它。下面用例子说明它的原理。

例 如果

$$uv=w^2,\ (u,v)=1,\ u>0,\ v>0$$

那么 u,v 都是平方数。

我们使用反证法，即证明：对于正整数u和v，使（1） u 和 v 互素；（2） uv 是平方数；（3） u 和 v 都不是平方数，是不可能的。

假设这样的 u 和 v 可以找到。如果需要的话，用交换u 和v，可以假设u 不是平方数。当然u 不是1。因而u 至少被一个素数整除。令P是整除 u 的素数，即 $u=Pk$，那么 $P|w^2$，得 $P|w$，即 $w=Pm$。因此 $uv=w^2$ 可以改写为 $Pkv=(Pm)^2=P^2m^2$，或 $kv=Pm^2$。因为 P整除右端，则 P整除左端。又$(P,v)=1$，则$P|k$，即$k=Pu'$.故有 $u'v=m^2$.因为 $u=Pk=P^2u'$，u'的任何因数是 u 的因数，所以 $(u',v)=1$．如果 u' 是平方数，那么 $u=Pu'$ 是平方数，与假设矛盾，故 u' 不是平方数。于是 u',v 也有以上

列举的性质（1）—（3），且 $u'<u$。然后，同样论证，有另外的正整数 $u''<u'$，使 u',v 有同样的三条性质。无限地重复论证，将得到无限递减的正整数序列 $u>u'>u''>\cdots>0$。这是不可能的，所以对于 u 和 v 具有三条性质是不可能的。这就证明了命题是真的。

（四）四次的费马方程

费马声称他已证明

$$x^4+y^4=z^4 \tag{1}$$

没有正整数解。但他没有写出证明过程，人们无法知道他采取什么具体方法。然而，我们可从那本《算术》书上另一处旁注的内容，应用一种微妙的技巧，轻而易举地证明（1）没有正整数解。

事实上，假设（1）有正整数解 x,y,z。令 $a=y^4$，$b=2x^2z^2$，$c=z^4+x^4$，$u=y^2xz$，则

$$a^2+b^2=y^8+b^2=(z^4-x^4)^2+4x^4z^4=(z^4+x^4)^2=c^2$$

又

$$\frac{1}{2}ab=y^4x^2z^2=(y^2xz)^2=u^2$$

因此，当 $a^2+b^2=c^2$时，$\frac{1}{2}ab=u^2$有正整数解。但费马已经证明无解。所以假设不成立，即（1）无正整数解。

费马讨论了勾股数组问题。他认为构成勾股数组的直角三角形的面积不可能是完全平方数，即

如果 $a^2+b^2=c^2$，a,b,c是正整数，则$\frac{1}{2}ab$ 不可能是完全平方数（或者说，$\frac{1}{2}ab=u^2$ 没有正整数解）。

费马在论证这个命题时，使用了他自己创造的无穷递降法。证明的过程大致是这样的：如果正整数 a,b,c,u满足 $a^2+b^2=c^2$，$\frac{1}{2}ab=u^2$，则能够找出另一组正整数 a_1,b_1,c_1，u_1，使得 $a_1^2+b_1^2=c_1^2$，$\frac{1}{2}a_1b_1=u_1^2$，且 $c>c_1$。这样过程可以无限地重复下去，得到一个严格无穷递降的正整数列

$$c>c_1>c_2>\cdots>c_n>\cdots>0$$

而 c 是一个确定的正整数，这是不可能的。因

此，假设不成立，从而证明命题是真的。

以上的证明也是不容易的。因此，后来的数学家便直接运用无穷递降法去证明（1）无正整数解。其证明思路如下：假设(x_0,y_0,z_0)是（1）的一个正整数解，那么存在同样性质的另一个解(x_1,y_1,z_1)，其中 $z_0>z_1$。因为这种过程可以无限的重复，所以得到严格无穷递减数列 $z_0>z_1>z_2>\cdots>0$，这是不合理的。因此，（1）没有正整数解。

实际上，人们证明了比 $n=4$ 情形 FLT 还强的定理。

定理1 方程

$$x^4+y^4=z^2 \qquad (2)$$

没有正整数解。

证明 令 (x,y,z) 是（2）的一个正整数解。不失一般，我们可以假设$(x,y,z)=1$，$2|y$。这样一来，(x^2,y^2,z)是一组基本勾股数。根据第二部分（二）中定理1，存在整数 $a,b,a>b>0$，$(a,b)=1$，a、b 奇偶性相反，且

$$\begin{cases} x^2=a^2-b^2 \\ y^2=2ab \\ z=a^2+b^2 \end{cases} \qquad (3)$$

容易看出，b 必为偶数。若 b为奇数，则 a为偶

数，因而 $4n+1=x^2=a^2-b^2=4m-1$，矛盾。

因为 $x^2+b^2=a^2$ 和 $(x,b,a)=1$，则由第二部分（二）中定理1，存在整数 c、d，$c>d>0$，$(c,d)=1$，c、d奇偶性相反，且

$$\begin{cases} x=c^2-d^2 \\ b=2cd \\ a=c^2+d^2 \end{cases} \tag{4}$$

因而

$$y^2=2ab=4cd(c^2+d^2) \tag{5}$$

因为 c,d,c^2+d^2 是两两互素的，根据素因数分解的唯一性，从（5）可知 c,d,c^2+d^2 都是正整数的平方：

$$\begin{cases} c=e^2 \\ d=f^2 \\ c^2+d^2=g^2 \end{cases} \tag{6}$$

于是

$$e^4+f^4=g^2 \tag{7}$$

即数组 (e,f,g)是（2）的解。

但是，$z=a^2+b^2=(c^2+d^2)^2+4c^2d^2$

$>g^4>g>0$。

根据无穷递降法原理，导致矛盾。定理得证．□

推论　方程

$$x^4+y^4=z^4 \tag{1}$$

没有正整数解。

证明 如果（1）有正整数解 x,y,z，那么方程

$$x^4+y^4=(z^2)^2$$

也有正整数解。根据定理1，这是不可能的，故（1）没有正整数解。□

一些四次的方程，类似于方程（2）用无穷递降法可以处理。我们引用下面定理：

定理2 下列方程没有正整数解：

$$x^4-y^4=\pm z^2 \qquad (8)$$

$$x^4+4y^4=z^2 \qquad \text{（欧拉）} \quad (9)$$

$$x^4-4y^4=\pm z^2$$

勒让德证明：

定理3 设x,y,z是非零的整数：

如果 $x^4+y^4=2z^2$，那么 $x^2=y^2$，且 $z^2=x^4$。

如果 $2x^4+2y^4=z^2$，那么$x^2=y^2$，且$z^2=4x^4$。

（五）三次的费马方程

在第一部分里已经提到，首先发表 $n=3$ 情形 FLT 的证明应归功于欧拉，它出现在1770年出版的欧拉的《代数》一书中。欧拉证明中的重

要步骤使用了 a^2+3b^2 型整数的可除性，但没有给出充分的理由。勒让德在他的书中（1830）重复了欧拉的证明，没有给出进一步的解释。因为在这个问题上他也是一位专家，当然通晓欧拉的推论。数学家对此发表了一系列文章。1966年波格曼发表了欧拉证明的彻底分析，出于历史的考虑，使这个争论更加明朗化。的确，1760年欧拉已经严格证明：如果 s是奇数，且 $s^3=a^2+3b^2$，其中 $(a,b)=1$，那么 $s=u^2+3v^2$，这里 u,v 是整数。

这个情形的另外一个证明是高斯给出的。两个证明都用无穷递降法，尽管欧拉用的 a^2+3b^2 型数，而高斯使用 $a+b\sqrt{-3}$ 型复代数数。下面我们还将看到，欧拉的证明只不过是高斯证明的一个特例，而后者的证明比前者要简单的多。

这里，首先给出一个初等证明，然后给出欧拉和高斯的证明。

1. 初等证明

引理1 方程

$$x_1x_2\cdots x_n=w^3 \qquad (1)$$

其中 $x_1,x_2,\cdots,x_n$ 两两互素， 全部整数解可由下列公式给出：

$$x_1=\alpha^3,\ x_2=\beta^3,\cdots,x_n=\tau^3,$$
$$w=\alpha\beta\cdots\tau \qquad (2)$$

其中 $\alpha,\beta,\cdots,\tau$ 两两互素。

证明　由（2）确定的 $x_1,x_2,\cdots,x_n$，w显然适合方程（1）。现证明方程（1）的每一个解都可表示为（2）形。设 x_1，x_2，…，x_n，w 为方程（1）的一个解。令

$$x_1=\alpha^3x_1',\ x_2=\beta^3x_2',\cdots,\ x_n=\tau^3x'_n \qquad (3)$$

其中 $x_1',x_2',\cdots,x_n'$ 为不含有立方因数的正数。因为 $x_1,x_2,\cdots,x_n$ 两两互素，所以 $\alpha,\beta,\cdots,\tau$ 及$x_1',x_2'\cdots,x_n'$ 都两两互素。从（1）知 $\alpha^3\beta^3\cdots\tau^3|w^3$，得 $\alpha\beta\cdots\tau|w$。设$w=\alpha\beta\cdots\tau w_1$，代入（1），得 $x_1'x_2'\cdots x_n'=w_1^3$。

如果 w_1 有素因数p，那么 $p^3|x_1'x_2'\cdots x_n'$。因为 $x_1',x_2',\cdots,x_n'$ 两两互素，所以 p^3 整除某个 x_i'，这与 x_i' 没有立方因数矛盾，因此只有 $w_1=1$。于是 $x_1'x_2'\cdots x_n'=1$。因为 x_i' 都是正整数，故 $x_1'=x_2'=\cdots=x_n'=1$。因此（3）为

$$x_1=\alpha^3,\ x_2=\beta^3,\cdots,x_n=\tau^3$$

其中 $\alpha,\beta,\cdots,\tau$ 两两互素。而 $w=\alpha\beta\cdots\tau$。□

引理2　方程

$$x^2+3y^2=z^3,\ (x,y)=1 \qquad (4)$$

的一切整数解可以表示为

$$\begin{cases} x = u^3 - 9uv^2 \\ y = 3u^2v - 3v^3 \\ z = u^2 + 3v^2 \end{cases} \tag{5}$$

其中 $(u,v)=1, 3\nmid u, u$、v 一奇一偶。

证明 略。

推论 1 方程

$$x^2 - xy + y^2 = z^3,\ (x,y)=1 \tag{6}$$

的一切整数解包含在下列两组公式中：

$$\begin{cases} x = u^3 + 3u^2v - 9uv^2 - 3v^3 \\ y = 6u^2v - 6v^3 \\ z = u^2 + 3v^2 \end{cases} \tag{7}$$

其中 $(u,v)=1, 3\nmid u$，u、v 一奇一偶；

$$\begin{cases} x = u^3 + 3u^2v - 9uv^2 - 3v^3 \\ y = u^3 - 3u^2v - 9uv^2 + 3v^3 \\ z = u^2 + 3v^2 \end{cases} \tag{8}$$

其中 $(u,v)=1$，$3\nmid u$，u、v一奇一偶。

推论 2 方程

$$x^2 - xy + y^2 = 3z^3,\ (x,y)=1 \tag{9}$$

的一切整数解均可由下面两组公式表出：

$$\begin{cases} x = u^3 + 9u^2v - 9uv^2 - 9v^3 \\ y = 2u^3 - 18uv^2 \\ z = u^2 + 3v^2 \end{cases} \tag{10}$$

其中 $(u,v)=1$，$3\nmid u$，u、v 一奇一偶。

$$\begin{cases} x=u^3+9u^2v-9uv^2-9v^3 \\ y=-u^3+9u^2v+9uv^2-9v^3 \\ z=u^2+3v^2 \end{cases} \qquad (11)$$

其中 $(u,v)=1$，$3\nmid u$，u、v 一奇一偶。

现在我们证明

定理 方程

$$x^3+y^3+z^3=0,\ (x,y)=1 \qquad (12)$$

没有非零的整数解。

证明 首先，我们证明方程（12）没有 $3\nmid xyz$ 解。若方程（12）有解 x,y,z，则

$$(x+y)(x^2-xy+y^2)=(-z)^3 \qquad (13)$$

如果 $(x+y)$ 与 (x^2-xy+y^2) 有素公因数 p，即 $p\mid(x+y)$，$p\mid(x^2-xy+y^2)$，那么由 $3xy=(x+y)^2-(x^2-xy+y^2)$ 推得 $p\mid 3xy$。由于 $3\nmid z$，故 $p\neq 3$，所以 $p\mid xy$，不防设 $p\mid x$，又因 $p\mid(x+y)$，则有 $p\mid y$，与 $(x,y)=1$ 矛盾。因此，$(x+y)$ 与 (x^2-xy+y^2) 互素。由（13）并根据引理 1，有

$$\begin{aligned} &x+y=\alpha^3 \\ &x^2-xy+y^2=\beta^3 \\ &-z=\alpha\beta \end{aligned} \qquad (14)$$

其中 $(\alpha,\beta)=1$。在（14）的第二式中，因 (x,y)

$=1$，$3\nmid x$，$3\nmid y$，根据引理 2 的推论 1 必有

$$\begin{cases} x=u^3+3u^2v-9uv^2-3v^3 \\ y=u^3-3u^2v-9uv^2+3v^3 \\ z=u^2+3v^2 \end{cases} \qquad (15)$$

其中$(u,v)=1$，$3\nmid u$，u、v一奇一偶。把（15）中的 x,y代入（14）第一式，得

$$2u(u+3v)(u-3v)=\alpha^3 \qquad (16)$$

因为 $(u,v)=1,3\nmid u$，u、v 一奇一偶，所以$2u$，$u+3v$，$u-3v$两两互素，再根据引理 1 必有

$$\begin{aligned} &2u=\alpha_1^3 \\ &u+3v=\beta_1^3 \\ &u-3v=\gamma_1^3 \\ &\alpha=\alpha_1\beta_1\gamma_1 \end{aligned} \qquad (17)$$

其中 $\alpha_1,\beta_1,\gamma_1$ 两两互素。由（17）的前三式消去 u,v，得

$$\alpha_1^3+(-\beta_1)^3+(-\gamma_1)^3=0 \qquad (18)$$

因为 $-z=\alpha\beta=\alpha_1\beta_1\gamma_1\beta$，所以 $3\nmid\alpha_1\beta_1\gamma_1$，且 $|z|>|\gamma_1|>0$。用同样方法又可得

$$\alpha_2^3+\beta_2^3+\gamma_2^3=0 \qquad (19)$$

其中 $\alpha_2,\beta_2,\gamma_2$ 满足 $3\nmid\alpha_2\beta_2\gamma_2$，$|\gamma_1|>|\gamma_2|>0$。继续进行下去，可得一无穷递减正整数序列

$$|z|>|\gamma_1|>|\gamma_2|>\cdots>0$$

这是不可能的。因此（12）没有 $3\nmid xyz$ 解。

其次，证明方程（12）没有 $3|xyz$ 解。

设 $z=3^n z_1$，$3\nmid z_1$，代入（12），得

$$x^3+y^3+3^{3n}z_1^3=0 \tag{20}$$

因为 x,y,z 两两互素，故 $3\nmid x$，$3\nmid y$。我们只需证明，对于任意 n，方程（20）无解即可。

对n施行归纳法：

当 $n=0$ 时，上面已经证明（20）没有解。假设 $n-1$时方程（20）没有解。若对n，(20) 有解 x,y,z_1，则

$$(x+y)(x^2-xy+y^2)=3^{3n}(-z_1)^3 \tag{21}$$

因为 $x^2-xy+y^2=(x+y)^2-3xy$，且 $3\nmid xy$，所以，若 $3\nmid(x+y)$，则 $3\nmid(x^2-xy+y^2)$；若 $3^s\|(x+y)$，其中 $s\geq1$，则 $3|(x^2-xy+y^2)$，而 $3^2\nmid(x^2-xy+y^2)$。由（21）必有 $3^{3n-1}|(x+y)$，$3\|(x^2-xy+y^2)$。按照前述方法，类似可证 $x+y$，x^2-xy+y^2 没有不等于 3 的素公因数，因而，$\frac{1}{3^{3n-1}}(x+y)$ 与 $\frac{1}{3}(x^2-xy+y^2)$互素。由方程（21）并根据引理 1，则有

$$\begin{aligned} x+y&=3^{3n-1}\alpha^3 \\ x^2-xy+y^2&=3\beta^3 \\ -z_1&=\alpha\beta \end{aligned} \tag{22}$$

其中$(\alpha,\beta)=1$。在（22）的第二式中，因为$(x,$

$y)=1$，根据引理的推论 2，必有

$$\begin{cases} x=u^3+9u^2v-9uv^2-9v^3 \\ y=2u^3-18uv^2 \\ z=u^2+3v^2 \end{cases} \qquad (23)$$

其中 $(u,v)=1$，$3\nmid u$，u、v 一奇一偶。

或者

$$\begin{cases} x=u^3+9u^2v-9uv^2-9v^3 \\ y=-u^3+9u^2v+9uv^2-9v^3 \\ z=u^2+3v^2 \end{cases} \qquad (24)$$

其中 $(u,v)=1$，$3\nmid u$，u、v一奇一偶. 将(23)的 x,y 代入 (22) 的第一式，得

$$u^3+3u^2v-9uv^2-3v^3=3^{3n-2}\alpha^3 \qquad (25)$$

因为$3\nmid u$，所以 (25) 式左端不被 3 整除. 于是 (25) 式不成立，故 (23) 式也不成立；再把 (24) 的 x,y 代入 (22) 的第一式，得

$$2v(u+v)(u-v)=3^{3(n-1)}\alpha^3 \qquad (26)$$

因为 $(u,v)=1$，u,v一奇一偶，所以$2v$，$u+v$，$u-v$ 两两互素. 因此它们中之一必被 $3^{3(n-1)}$ 整除. 不防设 $3^{3(n-1)}|(u-v)$. 根据引理 1，必有

$$\begin{aligned} 2v&=\alpha_1^3 \\ u+v&=\beta_1^3 \\ u-v&=3^{3(n-1)}\gamma_1^3 \end{aligned} \qquad (27)$$

$$\alpha=\alpha_1\beta_1\gamma_1$$

其中 $\alpha_1,\beta_1,\gamma_1$ 两两互素。因 $-z=\alpha\beta=\alpha_1\beta_1\gamma_1\beta$，故 $3\nmid\alpha_1\beta_1\gamma_1$。因此，得

$$\alpha_1^3+(-\beta_1)^3+3^{3(n-1)}\gamma_1^3=0 \tag{28}$$

这与归纳假设矛盾。如果 $2v$ 或 $u+v$ 被 $3^{3(n-1)}$ 整除，则分别得

$$(-\beta_1)^3+\gamma_1^3+3^{3(n-1)}\alpha_1^3=0 \tag{29}$$

或者

$$\alpha_1^3+\gamma_1^3+3^{3(n-1)}(-\beta_1)^3=0 \tag{30}$$

这些都与归纳假设矛盾。定理得证。□

2．欧拉的证明

这里介绍欧拉证明的概要。

证明 假设 x,y,z 是两两互素的整数，适合方程（12），其中 x,y 是奇数，z 是偶数，且 $|z|$ 是可能解中最小的。不失一般，这个假设是可以的。那么

$$\begin{aligned} x+y&=2a \\ x-y&=2b \end{aligned} \tag{31}$$

这里 a,b 是互素的非零整数，奇偶性相反。因此，

$$\begin{aligned} -z^3=x^3+y^3&=(a+b)^3+(a-b)^3 \\ &=2a(a^2+3b^2) \end{aligned} \tag{32}$$

容易推出 a^2+3b^2 是奇数，8 整除 $2a,b$ 是

奇数，且$(2a, a^2+3b^2)=1$ 或 3 。

情形Ⅰ　$(2a, a^2+3b^2)=1$。

从（32）及引理1可知，$2a$ 和 a^2+3b^2 都是某数的立方：

$$\begin{aligned} 2a &= r^3 \\ a^2+3b^2 &= s^3 \end{aligned} \tag{33}$$

这里 s 是奇数。在这一点上，按照欧拉的意思，把 s 表示成 $s=u^2+3v^2$ 是可能的，其中 u,v 使

$$\begin{aligned} a &= u(u^2-9v^2) \\ b &= 3v(u^2-v^2) \end{aligned} \tag{34}$$

于是 v 是奇数，$u\neq 0$，u 是偶数，$3\nmid u$，$(u, v)=1$，且

$$r^3=2a=2u(u-3v)(u+3v) \tag{35}$$

注意到$2u$，$u-3v$，$u+3$ 必两两互素，于是它们是整数的立方：

$$\begin{aligned} 2u &= -l^3 \\ u-3v &= m^3 \\ u+3v &= n^3 \end{aligned} \tag{36}$$

其中 l,m,n 不等于零（因为 3 不整除u）。于是

$$l^3+m^3+n^3=0 \tag{37}$$

其中 l 是偶数。此外，因为 $b\neq0$，$3\nmid u$：

$$|z^3| = |2a(a^2+3b^2)| = |l^3(u^2-9v^2)(a^2+3b^2)| \geqslant 3|l^3| > |l^3|$$

这与 $|z|$ 最小的假设矛盾。

情形 Ⅱ $(2a, a^2+3b^2)=3$。

令 $a=3c$，那么 $4|c$，$3\nmid b$。由（32）得

$$-z^3=6c(9c^2+3b^2)=18c(3c^2+b^2) \qquad (38)$$

这里 $18c$ 与 $3c^2+b^2$ 互素，$3c^2+b^2$ 是奇数，且不是 3 的倍数。

于是$18c$，$3c^2+b^2$ 都是整数的立方：

$$\begin{aligned} 18c &= r^3 \\ 3c^2+b^2 &= s^3 \end{aligned} \qquad (39)$$

其中 s 是奇数。同情形Ⅰ一样，$s=u^2+3v^2$，其中整数 u,v 使

$$\begin{aligned} b &= u(u^2-9v^2) \\ c &= 3v(u^2-v^2) \end{aligned} \qquad (40)$$

于是u 是奇数，v 是偶数，$v\neq0$，$(u,v)=1$，且 $2v$，$u+v$，$u-v$两两互素。从

$$\left(\frac{r}{3}\right)^3=2v(u+v)(u-v) \qquad (41)$$

得

$$\begin{aligned} 2v &= -l^3 \\ u+v &= m^3 \\ u-v &= -n^3 \end{aligned} \qquad (42)$$

因此，

$$l^3+m^3+n^3=0$$

其中 l,m,n 是非零的整数，l 是偶数。最后，

$$\begin{aligned}|z|^3&=18|c|(3c^2+b^2)\\&=54|v(u^2-v^2)|(3c^2+b^2)\\&=27|l|^3|u^2-v^2|(3c^2+b^2)\\&\geqslant 27|l|^3>|l|^3\end{aligned}$$

这与 $|z|$ 的最小选择矛盾。□

3. 高斯的证明

首先，我们介绍一些代数的基础知识。

我们把经常用到的几种数集用字母表示：

$\mathbf{Z}$ 表示全体整数的集。

$\mathbf{Q}$ 表示全体有理数的集。

$\mathbf{R}$ 表示全体实数的集。

$\mathbf{C}$ 表示全体复数的集。

设 $A=\{a,b,c,\cdots\}$。我们称 $a,b,c,\cdots$ 是A的元素。如果 a是集 A的元素，就说 a 属于A,记作 $a\in A$;如果 a 不是集 A 的元素，就说 a 不属于 A,记作$\notin A$。

设A,B是两个集。如果 A 的每一个元素都是B 的元素，那么就说 A 是 B 的子集，记作$A\subseteq B$。如果集 A 与 B 的元素完全一样，就

说集 A,B 相等，记作 $A=B$；否则，就说集A，B 不相等，记作 $A\neq B$。当 $A\subseteq B$，$A\neq B$ 时，叫A是 B的真子集，记作 $A\subset B$. 显然，$\mathbf{Z}\subset\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$。

（1）数环和数域

定义 设 S 是 $\mathbf{C}$ 的一个非空子集.如果对于 S 中任意两个数 a,b，$a+b$，$a-b$，ab都在 S 内，那么就说 S 是一个数环。

例如，数集 $\mathbf{Z},\mathbf{Q},\mathbf{R},\mathbf{C}$都是数环。

定义 设 F是一个数环。如果

(i) F 含有一个不等于零的数；

(ii)若$a,b\in F$，且$b\neq 0$，则$\dfrac{a}{b}\in F$，那么

就说 F是一个数域。

例如，数集$\mathbf{Q},\mathbf{R},\mathbf{C}$都是数域。但 $\mathbf{Z}$ 不是数域。

由于研究不定方程的需要，人们讨论了一些特殊的复数：

$$\mathbf{Q}(i)=\{a+bi\,|\,a,b\in\mathbf{Q}\}$$

$$\mathbf{Z}(i)=\{a+bi\,|\,a,b\in\mathbf{Z}\}$$

对于复数加法和乘法，$\mathbf{Q}(i)$ 是一个数域，$\mathbf{Z}(i)$ 是一个数环。$\mathbf{Z}(i)$ 中的复数叫复整数。为了区别起见，我们把通常的整数叫做有理整数.

显然，$Z\subset Z(i)$，$Q\subset Q(i)$，$Z(i)\subset Q(i)$。

我们需要 $Q(i)$ 中复整数具有有理整数一些性质，特别是唯一分解定理成立。为此，需要建立复整数的整除、互素和素数等概念。

设 $\alpha,\beta\in Q(i)$，$\beta\neq0$。如果存在 $r\in Q(i)$，使得

$$\alpha=\beta r$$

则说 β 整除 α，记作$\beta|\alpha$；否则，说 β不整除α，记作$\beta\nmid\alpha$。

整除 1 的复整数叫做单位数。显然，在 $Q(i)$ 中仅有 ±1，$\pm i$ 整除 1。

设复整数$\alpha=a+bi$。我们把$\overline{\alpha}=a-bi$ 叫做 α 的共轭数，$N(\alpha)=\alpha\overline{\alpha}=a^2+b^2$ 叫做 α 的范数。易知

$$N(\alpha)=\begin{cases}0, & \alpha=0,\\ 1, & \alpha\text{是单位数},\\ a^2+b^2>1, & \text{其他}.\end{cases}$$

设 e 是 $Q(i)$ 的单位数。如果复整数 α,β 满足

$$\alpha=\beta e$$

那么就说 α与β相结合（或相伴），记作 $\alpha\sim\beta$.

例如，因为 $3+2i=(2-3i)i$，所以 $(3+2i)\sim(2-3i)$。

对 $N(\alpha)>1$的 α的任何分解式

$$\alpha=\beta\gamma$$

都得出$N(\beta)=0$,或 $N(\gamma)=1$,就说 α是$Q(i)$的素数，常以 π 表示。

唯一分解定理 设 $N(\alpha)>1$。如果

$$\alpha=\pi_1\pi_2\cdots\pi_r=\pi_1'\pi_2'\cdots\pi_s',(r\geqslant 1,s\geqslant 1)$$

则有 $r=s$,且 $\pi_i\sim\pi_i'$, $i=1,2,\cdots,r$.

众所周知，i 是二次多项式 x^2+1的根，而且 x^2+1在有理数域上不能分解为两个一次多项式的乘积，我们把 x^2+1 称做在 Q 上不可约，i 叫做二次代数整数，$Q(i)$ 叫做 i 添加到Q上的一个二次扩张，或高斯数域。

一般地，如果 d是一个无平方因子的有理整数，则称$Q(\sqrt{d})$ 为二次域。$d=-3$时，$Q(\sqrt{-3})$是二次域，它有六个单位数：± 1，$\pm\frac{1}{2}(1+\sqrt{-3})$，$\pm\frac{1}{2}(1-\sqrt{-3})$。我们可以证明，$Q(\sqrt{-3})$中素因数唯一分解定理成立。

设 $\alpha,\beta,\gamma\in Q(\sqrt{-3})$。如果 $\gamma|\alpha-\beta$，则说 α,β对模 γ同余，记作 $\alpha\equiv\beta(\bmod\ \gamma)$。

现在我们转向高斯的证明。我们已经知道，为了证明

$$x^3+y^3+z^3=0$$

没有非零的整数解，欧拉不得不使用比较复杂的方法。然而，使用复整数的知识，高斯简单明了地证明更一般的方程

$$\alpha^3+\beta^3+\gamma^3=0$$

没有不全为零的代数整数解。就是说，欧拉的证明是高斯证明的特例。这个问题说明，证明较普遍的定理比证明特殊的情况来得容易，这种现象在数学里是常见的。

高斯使用 $a+b\zeta$ 型复数，这里 a,b 是有理整数，$\zeta=\frac{1}{2}(-1+\sqrt{-3})$是 1 的三次原根。

注 如果η 是方程

$$x^n-1=0$$

的根，就说 η是一个 n次单位根。$n=3$时，就说 η是一个三次单位根。三个三次单位根为：$\zeta=\frac{1}{2}(-1+\sqrt{-3})$，$\eta=\frac{1}{2}(-1-\sqrt{-3})$。由于 $\zeta^2=\eta$，$\zeta^3=1$，所以称ζ是一个三次单位原根。

令

$$A=\{a+b\zeta\ |a,b\in \mathbf{Z},\ \zeta=\frac{1}{2}(-1+\sqrt{-3})\}$$

用近世代数语言来说，A 是一个环，即二次域 $\mathbf{Q}(\sqrt{-3})$的代数整数环。A的单位数是±1，$\pm\zeta$，$\pm\zeta^2$，它们全是单位根。

因为在二次域 $Q(\sqrt{-3})$ 中素因数唯一分解定理成立，求 A 的元素的最大公因数是可能的，在可以相差一个单位数倍数意义下是唯一确定的。A 的元素叫做互素的，如果它们的最大公因数是单位数。

起着重要作用的元素是 $\lambda=1-\zeta=\frac{1}{2}(3-\sqrt{-3})$。$\lambda$ 是素元且 $3\sim\lambda^2$。

我们注意，由于 $3\sim\lambda^2$，如果 $\alpha\equiv\beta \pmod{\lambda}$，那么 $\alpha^3\equiv\beta^3 \pmod{\lambda^3}$。

模 λ 恰好存在三个同余类，即 0，1 和 -1 三类。

在高斯证明中，下列同余式是必需的：

引理 如果 $\alpha\in A$ 且 $\lambda\nmid\alpha$，那么

$\alpha^3\equiv\pm1 \pmod{\lambda^4}$。

这个证明是简单的。下面是高斯的定理：

定理 方程

$$x^3+y^3+z^3=0 \tag{43}$$

没有不全为零的代数整数解 $\alpha,\beta,\gamma\in A$。

注 代数整数的意义，参见第四部分。

证明 假设定理不真，不失一般，约去最大公因数，存在互素的 α,β,γ，使 $\alpha^3+\beta^3+\gamma^3=0$。从此得出 α,β,γ 也两两互素。因此可以假设 $\lambda\nmid$

α, $\lambda\nmid\beta$.

情形 1　$\lambda\nmid\gamma$.

因此，α,β,γ 在同余类 1 或 -1 里。于是 $\alpha\equiv\pm1 \pmod{\lambda}$，因此 $\alpha^3\equiv\pm1 \pmod{\lambda^3}$。类似地，$\beta^3\equiv\pm1 \pmod{\lambda^3}$，$\gamma^3\equiv\pm1 \pmod{\lambda^3}$。于是

$$0=\alpha^3+\beta^3+\gamma^3\equiv\pm1\pm1\pm1 \pmod{\lambda^3}$$

符号的组合给出 ±1 或 ±3．显然$0\not\equiv\pm1 \pmod{\lambda^3}$；如果 $0\equiv\pm3 \pmod{\lambda^3}$，那么 $\lambda^3\mid\pm3\sim\pm\lambda^2$，因而 $\lambda\mid\pm1$，λ 是单位数，矛盾。

情形 2　$\lambda\mid\gamma$.

令 $\gamma=\lambda^n\delta$，其中 $n\geqslant1$，$\lambda\nmid\delta$，$\delta\in A$，因此

$$\alpha^3+\beta^3+\lambda^{3n}\delta^3=0 \tag{44}$$

其中 $\alpha,\beta,\delta\in A$，$n\geqslant1$。

于是，满足下列性质 (P_n)：

(P_n)：存在 α,β，$\delta\in A$ 使 $\lambda\nmid\alpha$，$\lambda\nmid\beta$，$\lambda\nmid\delta$，α，β互素，α,β,δ 是下列方程的解：

$$x^3+y^3+w\lambda^{3n}z^3=0 \tag{45}$$

其中 w是单位数（在 (44) 中，$w=1$）。

证明的思想如下：指出如果 (P_n) 被满足，那么 $n\geqslant2$且 (P_{n-1})也被满足。重复这个过程，最后 (P_1) 被满足，这是个矛盾。这只不过是无穷递降法的一种形式（关于指数 n）。

于是，证明还剩下两步。

第一步。如果(P_n)被满足，那么 $n\geq 2$。

因为 $\lambda\nmid\alpha$，$\lambda\nmid\beta$，根据引理 $\alpha^3\equiv\pm 1 \pmod{\lambda^4}$，$\beta^3\equiv\pm 1 \pmod{\lambda^4}$，并且 $\pm 1\pm 1\equiv -w\lambda^{3n}\delta^3 \pmod{\lambda^4}$，其中 $\lambda\nmid\delta$。因为 $\lambda\nmid\pm 2$，左边必为0，因此 $3n\geq 4$，得$n\geq 2$。

第二步。如果 (P_n)被满足，那么 (P_{n-1})也被满足。

根据假设：

$$-w\lambda^{3n}\delta^3=\alpha^3+\beta^3=(\alpha+\beta)(\alpha+\zeta\beta)(\alpha+\zeta^2\beta). \tag{46}$$

素元 λ 必整除右边因子中的一个。因为$1\equiv\zeta\equiv\zeta^2 \pmod{\lambda}$，所以 $\alpha+\beta\equiv\alpha+\zeta\beta\equiv\alpha+\zeta^2\beta \pmod{\lambda}$，因此 λ整除每一个因子。于是

$$\frac{\alpha+\beta}{\lambda},\ \frac{\alpha+\zeta\beta}{\lambda},\ \frac{\alpha+\zeta^2\beta}{\lambda}\in A$$

并且

$$-w\lambda^{3(n-1)}\delta^3=\frac{\alpha+\beta}{\lambda}\cdot\frac{\alpha+\zeta\beta}{\lambda}\cdot\frac{\alpha+\zeta^2\beta}{\lambda} \tag{47}$$

从$n\geq 2$（由第一步）λ 整除右边因子中的一个。容易看出 $\alpha+\beta$，$\alpha+\zeta\beta$，$\alpha+\zeta^2\beta$ 模 λ^2 两两不同余。因此λ仅整除（47）式右边因子中的

一个。例如λ整除$(\alpha+\beta)/\lambda$（其他情形是类似的，用$\zeta\beta$或$\zeta^2\beta$代替β是允许的）。

于是$\lambda^{3(n-1)}$整除$(\alpha+\beta)/\lambda$。因此

$$\begin{aligned}\alpha+\beta&=\lambda^{3n-2}k_1\\ \alpha+\zeta\beta&=\lambda k_2\\ \alpha+\zeta^2\beta&=\lambda k_3\end{aligned}\tag{48}$$

其中$k_1,k_2,k_3\in A$，λ不整除k_1,k_2,k_3。

(48)中的三式边边相乘，得

$$-w\delta^3=k_1k_2k_3\tag{49}$$

容易看出k_1,k_2,k_3是两两互素的。因为环A有唯一分解，k_1，k_2,k_3与立方数有关

$$\begin{aligned}k_1&=\eta_1\varphi_1^3\\ k_2&=\eta_2\varphi_2^3\\ k_3&=\eta_3\varphi_3^3\end{aligned}\tag{50}$$

其中η_i是单位数，$\varphi_i\in A$ $(i=1,2,3)$，$\varphi_1,\varphi_2,\varphi_3$两两互素，$\lambda$不整除$\varphi_1,\varphi_2,\varphi_3$。于是

$$\begin{aligned}\alpha+\beta&=\lambda^{3n-2}\eta_1\varphi_1^3\\ \alpha+\zeta\beta&=\lambda\eta_2\varphi_2^3\\ \alpha+\zeta^2\beta&=\lambda\eta_3\varphi_3^3\end{aligned}\tag{51}$$

从$1+\zeta+\zeta^2=0$，得

$$\begin{aligned}0&=(\alpha+\beta)+\zeta(\alpha+\zeta\beta)+\zeta^2(\alpha+\zeta^2\beta)\\ &=\lambda^{3n-2}\eta_1\varphi_1^3+\zeta\lambda\eta_2\varphi_2^3+\zeta^2\lambda\eta_3\varphi_3^3\end{aligned}$$

于是

$$\varphi_2^3+\tau\varphi_3^3+\tau'\lambda^{3(n-1)}\varphi_1^3=0 \qquad (52)$$

这里 τ,τ' 是单位数，$\varphi_1,\varphi_2,\varphi_3\in A$ 不是 λ 的倍数，并且 φ_2,φ_3 互素。

如果 $\tau=1$，那么 $\varphi_2,\varphi_3,\varphi_1$ 是下列方程的解

$$x^3+y^3+\tau'\lambda^{3(n-1)}z^3=0 \qquad (53)$$

如果 $\tau=-1$，那么 $\varphi_2,-\varphi_3,\varphi_1$ 是（53）的解。

余下指出 $\tau\neq\pm\zeta$，$\pm\zeta^2$。实际上，因为 $n\geqslant 2$，

$$\varphi_2^3+\tau\varphi_3^3\equiv 0 \pmod{\lambda^4} \qquad (54)$$

但根据引理

$$\varphi_2^3\equiv\pm 1 \pmod{\lambda^4}$$

$$\varphi_3^3\equiv\pm 1 \pmod{\lambda^4}$$

因此 $\pm 1\pm\tau\equiv 0 \pmod{\lambda^2}$。

然而 $\pm 1\pm\zeta\not\equiv 0 \pmod{\lambda^2}$ 和 $\pm 1\pm\zeta^2\not\equiv 0 \pmod{\lambda^2}$。于是 $\tau\neq\pm\zeta$，$\pm\zeta^2$，这就建立性质 (P_{n-1})。□

另外一些三次或六次方程用类似的方法可以得到解决：

下列方程没有非零的整数解：

$$x^3+4y^3=1 \qquad (55)$$

$$x^6-27y^6=2z^3 \qquad (56)$$

$$16x^6-27y^6=z^3 \qquad (57)$$

$$x^3+y^3=3z^3 \qquad (58)$$

（六）五次的费马方程

两位著名的数学家狄利克雷和勒让德分享着证明五次的 FLT 荣誉。当时，年青的狄利克雷仅有二十岁，刚开始他光辉的生涯。古稀老人勒让德是著名的数论和分析学家。

1825年，狄利克雷在巴黎科学院宣读了一篇论文，宣布他已经证明 $n=5$时的FLT。然而，他忽略考虑可能情形之一。在此期间，勒让德独立地发现一个复杂的证明，而狄利克雷正在完善他的证明中余留的情形。

本质上，狄利克雷的证明使用了域 $K=Q(\sqrt{5})$的算术。叙述证明的细节太长，分别考虑两种情形即可。第一种情形是十分容易的。第二种情形用无穷递降法处理。

下面的引理在证明中是基本的技术工具：

引理 令 a,b 是不为零的互素整数，奇偶性相反，$5\nmid a$，$5\mid b$。如果

$$a^2-5b^2=\pm\left(\frac{1+\sqrt{5}}{2}\right)^e\left(\frac{f+g\sqrt{5}}{2}\right)^5 \tag{1}$$

（其中$e\geqslant 0$，f,g 是奇偶性相同的整数）那么存在互素且奇偶性相反的整数 $c,d,5\nmid c$，使得

$$\begin{aligned} a &= c(c^4+50c^2d^2+125d^4) \\ b &= 5d(c^4+10c^2d^2+5d^4) \end{aligned} \tag{2}$$

类似的引理也是必需的，如果$\frac{1}{4}(a^4-5b^2)$是（1）型。这些引理是域$K=Q(\sqrt{5})$中元素唯一分解成素元（直到单位）乘积的根据。

（七）七次的费马方程

用初等理论证明 FLT 的任何尝试，即不使用库麦的理想素因子理论，必须叙述 $n=7$ 情形阻止欧洲最优秀的数学家们的努力事实。因为他们探讨问题使用错误的方法和一些简单的思想，这些多半是费马发现的，而他们把它应用到全部情形。

1832年狄利克雷发表 $n=14$情形 FLT 的证明。这个结果较 $n=7$ 情形弱（每一个14次幂是7次幂，反之不行），证明在某种意义上表明对于 $n=7$ 情形失效。七年以后，1839年拉梅第一个发表 $n=7$ 情形的证明。证明是相当长的和需

要技巧．由于它已被库麦的证明所代替，一般说来不需要再去研究它了．

1840年，勒贝格发现比拉梅更简单的证明．他使用下列多项恒等式：

$$(X+Y+Z)^7-(X^7+Y^7+Z^7)$$
$$=7(X+Y)(Y+Z)(Z+X)[(X^2+Y^2+Z^2+XY+YZ+ZX)^2+XYZ(X+Y+Z)] \qquad (1)$$

柯西和刘维尔在转述1839年拉梅的论文时，指出另外一般多项恒等式．如果p是素数，$p>3$，那么

$$(X+1)^p-X^p-1=pX(X+1)(X^2+X+1)^\varepsilon G_p(X) \qquad (2)$$

这里

$$\varepsilon=\begin{cases}1, 当\ p\equiv-1 \pmod 6,\\ 2, 当\ p\equiv 1 \pmod 6,\end{cases}$$

$G_p(X)$是整系数多项式，不是X^2+X+1的倍数．

拉梅在1840年使用的恒等式是：如果m是奇数，那么

$$(X+Y+Z)^m-(X+Y-Z)^m-(X-Y+Z)^m-(-X+Y+Z)^m$$
$$=4mXYZ\sum_{\substack{a,b,c\geq 0\\ a+b+c=\frac{1}{2}(m-3)}}$$

$$\frac{(m-1)!}{(2a+1)!(2b+1)!(2c+1)!}X^{2a}Y^{2b}Z^{2c}$$

(3)

用如此复杂的工具，拉梅发表对于任意指数的 FLT 的“证明”．这是失败的，因为拉梅不正确地使用相当于在分圆整数环中唯一分解——这不是普遍的有效。

注 关于分圆整数知识参见第四部分。

对于指数 7，勒贝格证明中的主要步骤如下：

1．如果 x,y,z 是两两互素不为零的整数，使 $x^7+y^7+z^7=0$，根据（1）：

$$s^7=7vt \tag{4}$$

这里

$$s=x+y+z$$
$$u=x^2+y^2+z^2+xy+xz+yz$$
$$v=(x+y)(y+z)(z+x) \tag{5}$$
$$t=u^2+xyzs$$

2．于是 $v\neq0$，$s\neq0$，v 和 s 是偶数，u 是奇数，$t\equiv1 \pmod 4$，$(t,xyz)=1$，$(t,v)=1$。

3．t 是某个整数的14次幂且 $7\nmid t$。令 $t=q^{14}$，$q\mid u$，于是 $u=qr$。

4．$v=7^7p^7$，其中 p 是偶数，因此

$$(x+y)(x+z)(y+z)=7^{6}p^{7} \tag{6}$$

$$(x^{2}+y^{2}+z^{2}+xy+yz+zx)^{2}+xyzs=q^{14} \tag{7}$$

$$x+y+z=7pq^{2} \tag{8}$$

$$x^{2}+y^{2}+z^{2}+xy+xz+yz=qr \tag{9}$$

5．设 $r-\frac{1}{2}7^{3}p^{2}q^{3}=a$，$q^{2}=b$，$p^{2}=2^{m+1}c$，处理上述关系式，得

$$a^{2}=b^{4}-2^{2m}\times 3\times 7^{4}b^{2}c^{2}+2^{4(m+1)}\times 7^{7}c^{4} \tag{10}$$

这里 a,b,c 是奇数且互素。

6．根据（10）式推断出证明是不可能的。要对 m 进行归纳。作为事实的依据，实际上这步要比证明的其他部分长。

三　朴素的方法



在这部分里，我们介绍不使用一些复杂的方法处理 FLT.我们不应该轻视这些尝试，相反，它们显得十分精巧，并能帮助了解问题的本质困难。

我们所以把这些结果分类为“朴素的方法”，仅仅因为 FLT 的证明存在另外的水平。这里不准备就这方面知识作全面阐述，仅对几种方法加以介绍。

（一）巴罗和阿贝尔的关系式

巴罗（由巴罗表而著名）于1810年发现如下关系式；稍后的1823年阿贝尔也给出这些公式，在他给洪保的一封信中提到了它们。

定理1 如果 x, y, z 是两两互素的整数，满足 $x^p+y^p+z^p=0$，并且 $p(\neq 2)$不整除z，那么存在整数 t，t_1，使得

$$x+y=t^p, \frac{x^p+y^p}{x+y}=t_1^p, \quad z=-tt_1 \qquad (1)$$

此外，$p \nmid tt_1$，$(t, t_1)=1$，t_1 是奇数且$t_1>1$。

于是，如果两两互素的整数 x，y，z 都不是 p 的倍数且满足 $x^p+y^p+z^p=0$，那么如下的巴罗——阿贝尔关系式成立：

$$x+y=t^p, \quad \frac{x^p+y^p}{x+y}=t_1^p, \quad z=-tt_1$$

$$y+z=r^p, \quad \frac{y^p+z^p}{y+z}=r_1^p, \quad x=-rr_1 \qquad (2)$$

$$z+x=s^p, \quad \frac{z^p+x^p}{z+x}=s_1^p, \quad y=-ss_1$$

在上述表示式中，整数r，s，t，r_1，s_1，t_1不是p 的倍数，r_1，s_1，t_1 是奇数，$(t, t_1)=(r, r_1)=(s, s_1)=1$，并且 $(r, s, t)=(r_1, s_1, t_1)=1$。

(2)式可以改写为

$$x=-r^p+\frac{r^p+s^p+t^p}{2}=\frac{-r^p+s^p+t^p}{2}$$

$$y=-s^p+\frac{r^p+s^p+t^p}{2}=\frac{r^p-s^p+t^p}{2} \quad (3)$$

$$z=-t^p+\frac{r^p+s^p+t^p}{2}=\frac{r^p+s^p-t^p}{2}$$

阿贝尔又指出 $p|z$ 时类似（1）的一些关系式。阿贝尔给出（1823）：

定理2 如果 x，y，z 是两两互素的整数，满足$x^p+y^p+z^p=0$，$p(\neq 2)$ 整除z，那么存在整数 $n\geqslant 2$，t，r，s，t_1，r_1，s_1 使得

$$x+y=p^{p^{n}-1}t^p,\frac{x^p+y^p}{x+y}=pt_1^p,\ z=-p^n tt_1$$

$$y+z=r^p,\frac{y^p+z^p}{y+z}=r_1^p,\ x=-rr_1 \quad (4)$$

$$z+x=s^p,\frac{z^p+x^p}{z+x}=s_1^p,\ y=-ss_1$$

象以前一样，r，s，t，r_1，s_1，t_1 满足已经指出的同样性质。

（二）热尔曼的理论

热尔曼是法国女数学家，柯西和勒让德的同时代人，她与他们有通讯联系 她的定理由于大

人物的敬佩而受到欢迎。我们打算说明她的结果是如何漂亮和灵巧。它的核心是以下定理：

定理 令 p，q 是不同的奇素数，满足以下条件：

1. 对于任意整数k，$k^p \not\equiv p \pmod q$；
2. 若 x，y，z 是整数，并且

$$x^p+y^p+z^p\equiv 0 \pmod q$$

则 q整除 x，y或者 z。

那么对于指数 p，FLT第一种情形是真的。

定理的证明使用了巴罗——阿贝尔关系式。

热尔曼的著名定理如下（1823）：

定理2 如果 p是一个奇素数，使 $2p+1$也是素数，那么对于 p，FLT的第一种情形成立。

定理的证明是非常精采的，它仅涉及初等数论中的勒让德符号的计算和费马小定理，我们把它写出来，供读者欣赏。

证明 检验素数 p和 $q=2p+1$ 满足定理1的条件是十分容易的。

如果 $p\equiv a^p \pmod q$，计算勒让德符号，得

$$\pm 1=\left(\frac{a}{q}\right)\equiv a^{(q-1)/2}=a^p\equiv p \pmod q$$

于是 $p\equiv \pm 1 \pmod q$，这是不可能的。

其次，假设 $x^p+y^p+z^p\equiv 0 \pmod q$，和

$q \nmid xyz$。因为 $p=(q-1)/2$，应用费马小定理，则

$$x^p \equiv \pm 1 \pmod q$$

$$y^p \equiv \pm 1 \pmod q$$

$$z^p \equiv \pm 1 \pmod q$$

于是 $0=x^p+y^p+z^p \equiv \pm 1+1\pm 1 \pmod q$，这也是不可能的。

这就是证明！□

注 素数模 p的二次同余式可以写成

$$x^2 \equiv a \pmod p$$

当它有解时，我们就说 a是 p的平方剩余；否则，当它没有解时，我们就说 a是 p的平方非剩余。

勒让德符号$\left(\frac{a}{p}\right)$：假定 p是奇素数，$(a, p)=1$，我们规定

$$\left(\frac{a}{p}\right)=\begin{cases} +1, \text{当 } a \text{ 是 } p \text{ 的平方剩余；} \\ -1, \text{当 } a \text{ 是 } p \text{ 的平方非剩余。} \end{cases}$$

我们有

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$$

这样一个好的结果立即产生几个推广。实际上，使用同样的思想，不过用稍微详细的分析方法，勒让德证明如下结果：

定理 3 对于奇素数指数p，FLT 第一种情

形成立，只要下列数中之一也是素数：$4p+1$，$8p+1$，$10p+1$，$14p+1$，$16p+1$。

由于这个定理，热尔曼和勒让德的结果包含了所有素数 $p<100$，从而证实了对于这些素数的第一种情形。虽然它仅是第一种情形，但它仍表明较以前的种种尝试有相当大的前进，况且更由于早在1823年它就被证明。

这个方法毕竟有它的局限性，它的困难在于给出素数 p，使 $2kp+1$ 也是素数，当 k 是大数时。其次，方法对于第二种情形不起作用。

更现代的结果由克拉斯涅（1940）和笛内斯（1951）给出。克拉斯涅的方法同笛内斯的一样，都不完全是朴素的。实际上，他们使用了近代代数的成果。这里是克拉斯涅的定理。

定理 4 假设 p 是一个奇素数，h 是整数，使

1. $q=2hp+1$ 是素数；
2. $3\nmid h$；
3. $3^{h/2}<2hp+1$；
4. $2^{2h}\not\equiv 1 \pmod q$。

那么对于 p，FLT 第一种情形成立。

1951年笛内斯证明：

定理 5 如果 p 是一个奇素数，h 是整数，

不是 3 的倍数，$h\leqslant 55$，且使 $q=2hp+1$是素数，那么对于 p，FLT第一种情形成立。

（三）温特的定理

1894年，温特考虑一个由二项式系数组成的矩阵，给出 FLT 第一种情形的一个标准。但是，由于矩阵太大，他的标准使用起来十分不便。况且，较晚一些时候认识到它本质上等价于热尔曼的定理。然而，现在我们介绍它，是由于另外一些有趣的联系。

对于 $n\geqslant 2$，令W_n 是 $n\times n$ 矩阵的行列式：

$$W_n=\det\begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} \cdots & \binom{n}{n-1} \\ \binom{n}{n-1} & 1 & \binom{n}{1} \cdots & \binom{n}{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ \binom{n}{1} & \binom{n}{2} & \binom{n}{3} \cdots & 1 \end{pmatrix}$$

这是一个循环行列式。例如，$W_2=-3$，$W_3=2^2\times 7$，$W_4=-3\times 5^3$，$W_5=-3^7\times 5^3\times 17^3$。

导致温特定理的第一个结果如下：

定理1　令 $p\neq 2$，$q=2hp+1$ $(h\geqslant 1)$是素

数．那么存在整数 x，y，z 使 $q\nmid xyz$，并且

$$x^p+y^p+z^p\equiv 0 \pmod{q}$$

当且仅当 $q\mid W_{2h}$。

现在，温特的定理如下：

定理2 令 $p\neq 2$，$q=2hp+1$ $(h\geqslant 1)$是素数．如果 $q\nmid W_{2h}$ 并且 $p^{2h}\not\equiv 1 \pmod{q}$，那么对于指数 p，FLT 第一种情形成立。

由定理容易推出：

定理3 设 p 是一个奇素数，当 $2p+1$，$4p+1$，$8p+1$，$10p+1$，$14p+1$，$16p+1$ 之一为素数时，对于 p，FLT 第一种情形成立。

这说明温特定理与热尔曼的理论等价。

热尔曼定理的另外推论由范迪弗给出(1926)：

定理4 如果 p是一个奇素数，$q=2hp+1$ 是素数，$q\nmid W_{2h}$和$2h=2^v p^k$，这里 $p\nmid v$,$k\geqslant 0$，那么对于 p,FLT 第一种情形成立。

我们还不知道，对于每一个素数 p是否存在 $h>1$，使 $q=2hp+1$ 是素数而且 $q\nmid W_{2h}$。这是一个困难的问题。

最后，我们介绍温特行列式几个整除性质。

定理5

1．如果n是偶数，那么$W_n=-(2^n-1)u^2$，

其中 u是整数.

2. 如果 $d \mid n$,那么 $W_d \mid W_n$.

3. $W_n=0$,当且仅当 $6 \mid n$.

不寻常和更有趣的是下面的结果.

E· 雷麦于1935年证明:

定理6 如果 p 是奇素数,那么 W_{p-2} 是 $p^{p-2}q_p(2)$的倍数,这里

$$q_p(2)=\frac{2^{p-1}-1}{p}$$

根据费马小定理数 $q_p(2)$是整数,叫做费马商.

特别地,1909年外斐力什的定理说,如果对于p第一种情形不成立,那么$q_p(2)\equiv 0 \pmod{p}$. 作为推论,有

定理7 如果 $p^{p-1}\nmid W_{p-1}$,那么对于指数p FLT第一种情形是真的.

因此,决定 W_{p-1} 模 p^{p-1} 的剩余是重要的.

1959年卡利兹证明

定理8

$$W_{p-1}\equiv\prod_{a=1}^{p-2}[(1+a)^p-a^p-1]$$

$$\equiv p^{p-2}\prod_{a=1}^{p-2}\left(\sum_{s=1}^{p-1}(-1)^{s-1}\frac{a^s}{s}\right)(\bmod p^{p-1})$$

注 符号Σ，Π分别表示连加和连乘。例如：$a_1+a_2+\cdots+a_n=\sum_{i=1}^{n}a_i$，$a_1a_2\cdots a_n=\prod_{i=1}^{n}a_i$。

利用定理8，卡利兹改善E·雷麦的结果(1960)：

定理9 如果$p^{p+33}\nmid W_{p-1}$，那么对于指数p，FLT第一种情形是真的。

(四) 拾 零

在这里我们把许多不同类型的结果加以分类。根据这些推论，我们可以看见它们的作者享受解决FLT的乐趣，并且充分意识到它们的影响不限于解决FLT。还有，有时不仅是相当精美或简单的证明，而且有些结果的再发现还有更大的使用价值。

我们从几个整除性质开始。1931年马斯寿泰斯和波美证明以下结果：

定理1 如果 $p\equiv-1\pmod 6$和x，y，z是非零的整数，使 $x^p+y^p+z^p=0$，那么3整除x，y或者 z。

1946年，依恩柯利证明关于5的较弱提法：

定理2 如果 $p>2$，$p\not\equiv1$，$9\pmod{20}$和x，y，z 是非零整数，使 $x^p+y^p+z^p=0$，那么5整除 x，y或者 z。

另一些珍贵的结果如下。1969年，斯维斯塔克证明：

定理3 如果 $p>2$，x，y，z 是两两互素的正整数，$x^p+y^p=z^p$，那么 p 整除$\varphi(x)$，$\varphi(y)$或$\varphi(z)$（其中 φ 表示欧拉*totient*函数）。

1913年，哥德兹海证明如下结果：

定理4 正整数 x，y，z 成算术级数时，它们不满足 $x^n+y^n=z^n$（其中 $n>2$）。

劳证明：

定理5 如果 $n>2$是奇素数，x，y，z 是正整数，使 $x^n+y^n=z^n$，那么$\mu(x+y)=0$（μ 表示莫比乌斯函数）。

注 莫比乌斯函数：

$$\mu(a)=\begin{cases}1, & \text{若 } a=1;\\ (-1)^r, & \text{若 } a\text{是 } r \text{ 个不同素数的乘积;}\\ 0, & \text{若 } a \text{ 被一个素数的平方整除。}\end{cases}$$

这里是 FLT 的几个等价提法。它们于1946年由培利兹——卡绍给出。条件（1），（2）和（3）等价于1901年由本兹首先证明，1978年由绍拉重复证明。

定理 6 令 $m \geqslant 2$，$n = 2m - 1$。那么下列提法是等价的：

1．方程 $X^n + Y^n = Z^n$ 在**Z**中仅有平凡解。

2．方程 $X(1+X) = T^n$ 在 **Q** 中仅有平凡解。

3．方程 $X^2 = 4Y^n + 1$在 **Q**中仅有平凡解。

4．方程 $X^2 = Y^{n+1} - 4Y$ 在 **Q** 中仅有平凡解。

5．对于每一个有理数a，多项式$Z^2 - a^m Z + a$ 在 **Q** 上不能分解。

6．方程 $(XY)^m = X + Y$在 **Q** 中仅有平凡解。

7．方程$X^m = (X/Y) + Y$ 在**Q** 中仅有平凡解。

8．如果 u_1，r 是非零有理数，u_1，u_2，$\cdots$ 是公比为 r的几何级数，那么 $u^2_m - u_1 + r \neq 0$。

9．如果$\triangle ABC$ 是直角三角形，$\angle CAB = 90°$，$AB = 2$，$AB + BC$ 是某个有理数的 n 次幂，那么 AC不是有理数。

此外，这些条件意味着：

10．抛物线 $Y^2=4X$ 在每一个不同于原点的有理点的切线，相交于曲线 $Y=X^m$ 的无理点。

最后，我们介绍惠维兹一篇极好的文章（1908）。他考虑丢番图方程

$$X^mY^n+Y^mZ^n+Z^mX^n=0 \qquad (1)$$

这里 $m\geqslant n$，$(m,n)=1$（不失一般），他证明

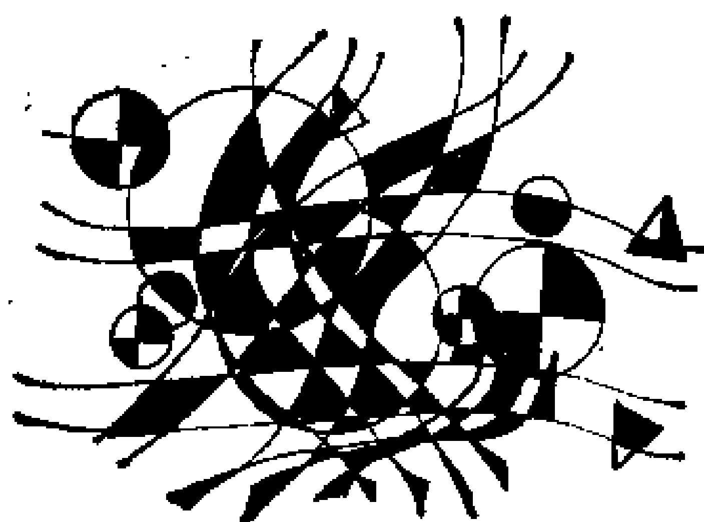
定理7　方程（1）仅有平凡解，当且仅当对于指数 m^2-mn+n^2，FLT 是真的。

例如，令 $m=3$，$n=1$，得到

$$X^3Y+Y^3Z+Z^3X=0$$

仅有平凡解．因为 $m^2-mn+n^2=7$，所以 $p=7$ 时 FLT 是真的。

四　代数数论方法



代数数论的形成和发展主要是由于不定方程的推动。我们在第二部分（五）里已经介绍了由高斯建立的复整数理论，它是代数数论发展方向上的一个阶段。库麦把高斯的理论推广到代数数，进而建立理想数的理论，为代数数论的产生奠定了基础。后来经戴德金、克罗内克和希尔伯特等人的发展和完善，目前代数数论已成为数学中内容异常丰富的分支，是研究不定方程的重要工具。

这里介绍代数数论的基础知识，特别是分圆域的知识，库麦的重要工作都是有关分圆域的。以及库麦利用分圆域的理论在解决 FLT 上做出的重大贡献。

定义 如果复数 θ是一个 n次整系数多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

的根，且 $f(x)$ 在 $\mathbf{Q}$ 上不可约，就把θ 叫做一个n 次代数数。如果$a_n=1$,则把 θ 叫做一个n次代数整数。

注　如果$f(x)$不能分解为两个次数比n 低的系数为有理数的多项式的乘积，则把$f(x)$ 叫做在$\mathbf{Q}$上不可约。

定义　设θ 是一个 n次代数整数，形如

$$a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}, a_i\in\mathbf{Q}, i=1, 2, \cdots, n-1$$

的数全体组成一个域，称为 θ 添加到 $\mathbf{Q}$ 上的一个 n次代数扩张，记作$\mathbf{Q}(\theta)$。$\mathbf{Q}(\theta)$ 中的全体代数整数组成一个数环，记作$\mathbf{Z}(\theta)$。

类似 $\mathbf{Q}(i)$ 的情形，我们建立 $\mathbf{Q}(\theta)$的分解定理。

设代数整数 α, $\beta\in\mathbf{Q}(\theta)$。若存在一个代数整数 γ，使得

$$\alpha=\beta\gamma$$

就说 β 整除 α，记作 $\beta\mid\alpha$；否则，就说 β不整除 α，记作 $\beta\nmid\alpha$。

设 α 是 $\mathbf{Q}(\theta)$的一个代数整数。如果α^{-1} 也是代数整数，就说 α 是 $\mathbf{Q}(\theta)$ 的一个单位数。

若代数整数α，β仅差一个单位因子，就说α与 β 相结合（或相伴）。

对于非单位代数整数 $\alpha\in\mathbf{Q}(\theta)$，如果有代数

整数 β，$\gamma\in Q(\theta)$，并且都不是单位数，使

$$\alpha=\beta\gamma$$

就说 α在 $Q(\theta)$中可分解；否则，就说 α是$Q(\theta)$的素元，或不可分解。

$Q(\theta)$ 的任一非单位数的代数整数可分解为素元的乘积。

我们知道$Z(i)$中唯一分解定理成立。但是，对一般的$Z(\theta)$却未必如此。例如，在$Z(\sqrt{-3})$中唯一分解定理成立，而在$Z(\sqrt{-5})$中，整数

$$6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$$

不难验证$2,3,1+\sqrt{-5},1-\sqrt{-5}$都是$Q(\sqrt{-5})$中的素元，并且2，3不能与 $1+\sqrt{-5}$，$1-\sqrt{-5}$相结合，故6的分解不唯一。

现在来看

$$\eta=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$$

η 是一个 p次单位根，又是Q上的 $p-1$次不可约多项式 $x^{p-1}+x^{p-2}+\cdots+x+1$ 的根，数域$Q(\eta)$叫做分圆域。可以证明，$Z(\eta)$ 由所有形如

$$c_0+c_1\eta+\cdots+c_{p-2}\eta^{p-2}$$

的数组成，其中c_0，c_1，…，c_{p-2} 取有理整数。

根据简单的代数知识，在 $Z(\eta)$ 中，费马方程 $x^p+y^p=z^p$ 可通过因式分解表示为

$$(x+y)(x+\eta y)\cdots(x+\eta^{p-1}y)=z^p$$

这时要是唯一分解定理成立，问题就好办了。实际上，$Z(\eta)$ 中唯一分解定理并不对所有 η 都一定成立。为了弥补这一情形，库麦引进了理想数。

现在我们回到一般的 n 次代数扩张 $Q(\theta)$。设 α_1，α_2，…，α_m 是 $Z(\theta)$ 中任意给定的m个代数整数，η_1，η_2，…，η_m 是 $Z(\theta)$ 中任意代数整数，我们把所有形如

$$\eta_1\alpha_1+\eta_2\alpha_2+\cdots+\eta_m\alpha_m$$

的数所组成集合叫做 $Z(\theta)$ 的一个理想数，记作 $[\alpha_1, \alpha_2, \cdots, \alpha_m]$，并把它看成是一个“数”。特别，$[\alpha]$叫做主理想数，$[1]$叫做单位理想数，$[0]=\{0\}$叫做零理想数。

设 $A=[\alpha_1, \alpha_2, \cdots, \alpha_m]$，$B=[\beta_1, \beta_2, \cdots, \beta_n]$，那么

$$AB=[\alpha_1\beta_1, \cdots, \alpha_m\beta_1, \cdots, \alpha_1\beta_n, \cdots, \alpha_m\beta_n]$$

叫做理想数A和B的乘积。

设 $A\neq[0]$，B 是两个理想数。若至少有一个理想数 C，使得

$$B=AC$$

则称A整除B，或称A是B的因数，记作$A\mid B$。

若理想数A除了本身和单位理想数〔1〕外，没有其它因数，则称A为素理想数。

库麦证明，$Z(\theta)$ 中任一不同于〔0〕和〔1〕的理想数 A，可以唯一地分解成素理想数的乘积。例如，前面提到$Z(\sqrt{-5})$ 的6，它的分解不唯一。但相应的理想数〔6〕却可以唯一分解成

$$[6]=[2,1+\sqrt{-5}]^2[3,1+\sqrt{-5}][3,1-\sqrt{-5}]$$

设 α，β 是 $Z(\theta)$ 的代数整数。若 $A|[\alpha-\beta]$，则称 α 和 β 对模 A 同余，记作 $\alpha\equiv\beta \pmod{A}$。

根据同余关系可以将 $Z(\theta)$ 的全体代数整数模A进行分类，称为模 A 的剩余类。

设 A，B 是 $Z(\theta)$ 的理想数。如果有$Z(\theta)$的主理想数$[\alpha]$和 $[\beta]$，使

$$[\alpha]A=[\beta]B$$

则称 A，B 属于同一理想数类，记作$A\sim B$。

由此，可以将 $Z(\theta)$ 的全体理想数进行分类，称为理想数类，其类数有限，记作h。库麦把 h 写成 $h=h^*h^+$，h^* 叫做第一个因数，h^+叫做第二个因数，这里

$$h^*=\frac{1}{(2p)^{(p-3)/2}}\left|G(\eta)G(\eta^3)\cdots G(\eta^{p-2})\right|$$

$$h^{+}=\frac{2^{(p-3)/2}}{R}\prod_{k=1}^{(p-1)/2}\left|\sum_{j=1}^{(p-3)/2}\eta^{2kj}\log\left|1-\zeta^{g^{j}}\right|\right|$$

上面公式中，η 是1的 $p-1$ 次原根；g 是模 p 原根；对于每一个 j，g_j 为 $1\leqslant g_j\leqslant p-1$ 并且 $g_j\equiv g^j \pmod p$，$G(x)=\sum_{j=0}^{p-2}g_jx^j$，$R$ 是分圆域的调整子，即与域的单位联系是固定不变的。

设 $\mathbf{Z}(\theta)$ 的类数为 h，p是任意奇素数。如果 $p\mid h$，则叫 p 为正规素数；如果 $p\nmid h$，则叫 p为非正规素数。

库麦利用理想数论的知识，成功地证明：

定理 当 p 是正规素数时，方程

$$x^p+y^p=z^p$$

没有正整数解，其中 x，y，z 两两互素。

关于正规素数的个数是有限还是无限，这也是没有解决的问题。但是，对于给定的素数 p，我们有办法判断它是否是正规素数。

定义 贝努利数 B_m $(m=1, 2, \cdots)$ 为

$$\frac{t}{e^t-1}=1-\frac{t}{2}+\sum_{m=1}^{\infty}\frac{(-1)^{m-1}B_mt^{2m}}{(2m)!}$$

不难计算：

$$B_1=\frac{1}{6},\ B_2=\frac{1}{30},\ B_3=\frac{1}{42},\ B_4=\frac{1}{30},$$

$$B_5=\frac{5}{66},B_6=\frac{691}{2730},\ B_7=\frac{7}{6},\ B_8=\frac{3617}{510},$$

$$B_9=\frac{43867}{798},B_{10}=\frac{174611}{330},B_{11}=\frac{854513}{138},$$

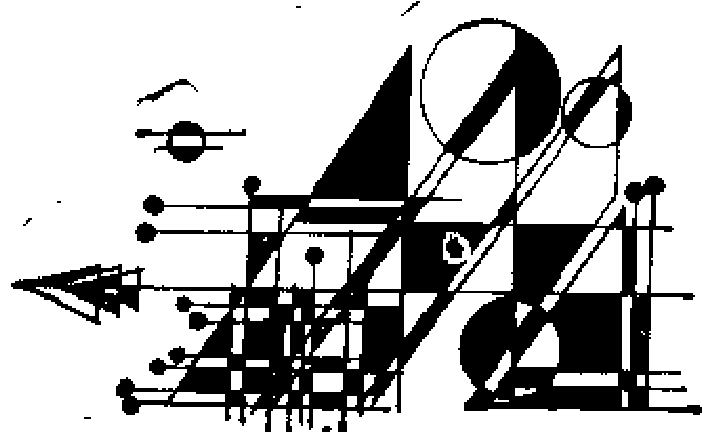
$$B_{12}=\frac{236364091}{2730},\ \cdots\cdots$$

库麦证明：设 $p>3$，如果素数 p 不整除前 $\frac{1}{2}(p-3)$ 个贝努利数的每一个数的分子，则 p 是正规素数。

用这个方法可以判定，对于小于 100 的奇素数，除37，59，67外，都是正规素数。因此，由上述定理可知，对于小于100的奇素数 p，FLT 成立。这就是库麦1847年的结果。

我们只要回顾一下库麦以前在 FLT 证明上的缓慢进程，就可以看出库麦的结果在当时是多么了不起的成就！

五　新近的成果



从第二部分和第三部分我们看到，在FLT的早期研究中，使用的方法大多是初等的或朴素的。但是，有关 FLT 的重要和深刻的结果，都是使用近代数学知识得到的。因此，在下面两部分近代成果说明中，我们将假定读者已经有一定的现代数学基础，在用到有关方面的知识时，就不作解释了。这里我们仅就各种结果作一个大概介绍，证明就不写了，有兴趣的读者可去查有关资料。

在这部分里，我们介绍几种新方法。这方面的内容较多，要介绍的方法是经过挑选的。

（一）$p<125000$费马猜想成立

我们在第一部分（七）里已经提到，对于每

一个素指数 $p<125000$ FLT是真的。这里要介绍它是如何得来的。

自然这个结果的证明是使用现代计算机做出的，这是瓦格斯塔夫坚持不懈工作的结果。他做这项工作时，使用IBM 360/65计算机，也使用IBM 370计算机。虽然这些计算机没有现在高级进步机器的速度和特性，但是无论如何计算机的使用，方法的应用都是十分可信赖的，因而结果是不成问题的。

在开始阐明方法以前，让我们回顾一下历史情况。

1847年库麦证明他的主要定理时，承认37是最小的非正规素数，指数 $p<37$ FLT得证。在他的1857年论文中，库麦证明定理，保证若干类非正规素数FLT成立。应用他的规则到小于100的非正规素数 $p=37$，59，67，他推断对于所有 $p<100$ FLT成立。可是，1920年范迪弗指出库麦1857年的证明存在一些缺陷。他在1926年补救了这些缺陷，并证明 $p<157$ FLT成立。

1929年范迪弗发表长篇论文，这里他给出几个新的标准。令 ζ 是1的 p 次原根，$K=\boldsymbol{Q}(\zeta)$，并令 A 是 K 的整数环。

定理1 假设

Ⅰ. K的类数的第二个因子 h^+ 不是 p 的倍数。

Ⅱ. 设有一个贝努利数 B_{2np} $(n=1, 2, \cdots (p-3)/2)$的分子是p^3 的倍数。

那么对于指数p，FLT 第二种情形是真的。

上面的标准不易应用，因为第二因子h^+的计算是很复杂的。

下列的标准更为实用：

定理2 假设

Ⅲ. 存在一个且仅一个下标$2s$，$2\leqslant 2s\leqslant p-3$，使 p 整除 B_{2s} ($p\mid B_{2s}$ 指 p 整除 B_{2s} 的分子，下同）。

Ⅳ. 对于上面的下标 $2s$，p^3 不整除 B_{2sp}。

那么对于指数 p，FLT 成立。

所有非正规素数 $p<221$，除157外，都包含在上面的标准中。

范迪弗的第三个定理是：

定理3 如果 $p\equiv 1 \pmod 4$和对于每一个奇数下标 s，$2\leqslant 2s\leqslant p-3$，$p\nmid B_{2s}$，那么对于指数 p，FLT 成立。

这个标准不满足157，因为157 整除 B_{62} 和 B_{110}. 应用到素数157的仅是他的第四个定理。我们采用下面的注记。令a_1，a_2，$\cdots$，a_t 是下标，

使 $1 \leqslant a_i \leqslant (p-3)/2$ 并且 $p \mid B_{2a_i}$。令 g 是模 p 的原根，σ 是 $K = \mathbf{Q}(\zeta)$ 的自同构，使 $\sigma(\zeta) = \zeta^g$。令

$$\delta = \sqrt{\frac{1-\zeta^g}{1-\zeta} \cdot \frac{1-\zeta^{-g}}{1-\zeta^{-1}}}$$

和对于 $a = 1, 2, \cdots, (p-3)/2$,

$$\theta_a = \prod_{i=0}^{(p-3)/2} \sigma^i \left(\delta^{g^{-2ia}}\right).$$

定理 4 假设

Ⅴ. 存在一个素数 l, $l \equiv 1 \pmod p$, $l < p^2 - p$, 使得如果 $1 \leqslant a_i \leqslant (p-3)/2$, $p \mid B_{2a_i}$, 那么单位 θ_{a_i} 与 $K = \mathbf{Q}(\zeta)$ 的某个整数的 p 次幂不同余，模 L，这里 L 是整除 Al 的素理想。

那么对于指数 p，FLT成立。

使用这个定理，在同一篇文章中范迪弗证明更实用的标准。

定理 5 假设

Ⅵ. 存在一个素数 l, $l \equiv 1 \pmod p$, $l \not\equiv 1 \pmod{p^2}$, 使同余式

$$X^p + Y^p + Z^p \equiv 0 \pmod l$$

仅有平凡解。

Ⅶ. 对于上面的素数 l，如果 $1 \leqslant a_i \leqslant (p-3)/2$, $p \mid B_{2a_i}$, 那么

$$\left\{ \frac{\theta_{ai}}{L} \right\} \neq 1$$

这里L是整除 Al 的 $K=\mathbf{Q}(\zeta)$ 的素理想，$\{-\}$表示 p 次幂剩余符号。

那么对于指数 p，FLT成立。

最后，这是可以应用到 $p=157$ 的第一个标准。

范迪弗也断定，对于每一个 $p<211$，h^+ 不是p的倍数。

1930年，用同样的方法，范迪弗证明对于每一个素数p，$211<p<269$，FLT 成立。1931年推广到307，1937年范迪弗和他的助手们又推进到617。在这点上，用台式计算机来计算是十分艰苦的工作。

在1954年的一篇重要论文中，D· H· 雷麦、E· 雷麦和范迪弗采用了更适于计算的新标准。

下面的引理是基础：

引理 令 l是一个素数，$l=kp+1<p^2-p$。令 t 是自然数，使 $t^k\not\equiv 1 \pmod{l}$。对于$a\geq 1$，令

$$d=\sum_{j=1}^{(p-1)/2} j^{p-2a} \text{ 和 } \theta_a=\frac{1}{t^{kd/l}}\prod_{i=1}^{(p-1)}(t^{ki}-1)^{i^{p-1-2a}}$$

用已经采用的符号，单位θ_a与$K=\mathbf{Q}(\zeta)$中某

个整数的 p次幂同余，模整除 Al 的素理想 L，当且仅当$\mathscr{A}^{ak}\equiv 1 \pmod{l}$。

使用这个引理，D·H·雷麦，E·雷麦和范迪弗证明下列标准：

定理6 假设 p 是一个非正规素数，令a_i，$1\leqslant a_i\leqslant(p-3)/2$，是下标，使 $p\mid B_{2a_i}$。用上面的符号，如果对于以上所有的下标 a_i，$2^k\not\equiv 1 \pmod{l}$和$\mathscr{A}^k_{a_i}\not\equiv 1 \pmod{l}$，那么对于指数$p$，FLT成立。

使用 SWAC 计算机，上面的作者证明，对于每一个指数 $p<2003$ FLT 成立。不久之后（1954），范迪弗又推进到2521。

这仅是许多数学家计算出一长串结果的开始。下面开列部分数学家计算出的结果和时间：

谢尔弗力基，尼可和

范迪弗，	$p<4002$，1955年。
谢尔弗力基和波劳克，	$p<25000$，1967年。
柯别列夫，	$p<5500$，1970年。
约翰逊，	$p<30000$，1975年。
瓦格斯塔夫，	$p<58150$，1975年。
瓦格斯塔夫，	$p<100000$，1976年。
瓦格斯塔夫，	$p<125000$，1977年。

（二）欧拉数和费马猜想

贝努利数与另外一种数宛如兄弟，欧拉在正割函数级数展开式中首先考虑了它：

$$\sec x = 1 - \frac{E_2}{2!}x^2 + \frac{E_4}{4!}x^4 - \frac{E_6}{6!}x^6 + \cdots$$

（对于 $|x| < \frac{\pi}{2}$ 收敛）　　（1）

上面展开式中的 E_n 叫做欧拉数。正象贝努利数一样，它们被广泛地研究过。

例如，它们满足基本的递推关系：

$$E_{2n} + \binom{2n}{2n-2}E_2 + \binom{2n}{2n-4}E_4 + \cdots + \binom{2n}{2}E_{2n-2} + 1 = 0 \quad (2)$$

于是，

$E_2 = -1$，$E_4 = 5$，$E_6 = -61$，$E_8 = 1385$，$E_{10} = -50521$，$E_{12} = 2702765$，$E_{14} = -199360981$，$E_{16} = 19391512145$，$E_{18} = -2404879675441$，$E_{20} = 370371188237525$，等。

通常也写

$E_0 = 1$，$E_{2n+1} = 0$，对于 $n \geq 0$。

容易看出欧拉数是整数。此外可以证明，对

实上它们是奇整数，有着交错的符号，并且它们的最后一个数字交错为1，5。

更有用的是建立它们与贝努利数间的关系。1825年色克指出：

$$E_{2k}=1-\sum_{i=1}^{k}\binom{2k}{2i-1}\frac{2^{2i}(2^{2i}-1B_{2i}}{2i}$$

$$=\frac{1}{2k+1}\left[1-\sum_{i=1}^{k}\binom{2k+1}{2i}2^{2i+1}(2^{2i-1}-1)B_{2i}\right] \qquad (3)$$

另一方面，

$$B_{2k}=\frac{2k}{2^{2k}(2^{2k}-1)}\left[\sum_{i=1}^{k-1}\binom{2k-1}{2i}E_{2i}+1\right] \qquad (4)$$

素数整除若干贝努利数与 FLT 的真实性间的联系，提示我们用欧拉数建立类似的理论。

素数 p 叫做 E—正规数，如果 p不整除欧拉数 E_2，E_4，…，E_{p-3}。

1940年，范迪弗证明：

定理1 如果p 不整除 E_{p-3},那么对于指数p,FLT第一种情形成立。

因此，如果 p是 E-正规数，上述结论仍然是真的。

在证明中使用的基本事实是1938年 E. 雷麦

得到的同余式：

$$\sum_{j=1}^{[p/4]}\frac{1}{j^2}\equiv\sum_{j=1}^{[p/4]}j^{p-3}\equiv(-1)^{(p-1)/2}4E_{p-3}\pmod{p} \quad (5)$$

在1954年关于非正规素数论文中，卡利兹也指出：

定理2 存在无穷多E－非正规素数p，即$p|E_2E_4\cdots E_{p-3}$。

但是，我们不知道是否存在无穷多E－正规素数。

最后，我们再列举两个结果：

定理3 存在无穷多E—非正规素数p，使$p\not\equiv1\pmod 8$。

定理4 如果存在x，y，z，使$p\nmid xyz$并且$x^{2p}+y^{2p}=z^{2p}$，那么p整除E_{p-3}，E_{p-5}，E_{p-7}，E_{p-9}，E_{p-11}，其中p是奇素数。

（三）莫德尔猜想

1983年，联邦德国数学家伐尔廷斯证明了莫德尔猜想，从而翻开了数论的新篇章。

伐尔廷斯于1954年7月28日生于联邦德国的

杰尔森柯琛，并在那里渡过了学生时代，而后就学于内斯涛德教授门下学习数学。1978年获得博士学位。他作过研究员、助教，现在是乌珀塔尔的教授。他在数学上的兴趣开始于交换代数，以后转向代数几何。

1922年，英国数学家莫德尔提出一个著名猜想，人们叫做莫德尔猜想。按其最初形式，这个猜想是说，任一不可约、有理系数的二元多项式，当它的“亏格”大于或等于2时，最多只有有限个解。记这个多项式为 $f(x, y)$，猜想便表示：最多存在有限对数偶 x_i，$y_i \in Q$，使得 $f(x_i, y_i)=0$。

后来，人们把猜想扩充到定义在任意数域上的多项式，并且随着抽象代数几何的出现，又重新用代数曲线来叙述这个猜想了。因此，伐尔廷斯实际上证明的是：任意定义在数域K上，亏格大于或等于2的代数曲线最多只有有限个K—点。

数学家对这个猜想给出各种评论，总的看来是消极的。

1979年利奔波姆说：“可以有充分理由认为，莫德尔猜想的获证似乎还是遥远的事。”

对于“猜想”，1980年威尔批评说：“数学家常常自言自语道：要是某某东西成立的话，‘这

就太棒了'(或者'这就太顺利了')．有时不用费多少事就能够证实他的推测，有时则很快否定了它。但是，如果经过一段时间的努力还是不能证实他的预测，那么他就要说到'猜想'这个词，既便这个东西对他来说毫无重要性可言。绝大多数情形都是没有经过深思熟虑的。”因此，对莫德尔猜想，他指出：我们稍许来看一下“莫德尔猜想”．它所涉及的是一个算术家几乎不会不提出的问题；因而人们得不到对这个问题应该去押对还是押错的任何严肃的启示。

然而，时隔不久，1983年伐尔廷斯证明了莫德尔猜想，人们对它有了全新的看法。在伐尔廷斯的文章里，还同时解决了另外两个重要猜想，即台特和沙伐尔维奇猜想，它们同莫德尔猜想具有同等重大意义。

这里主要解释一下莫德尔猜想，至于证明就不多讲了。

所谓代数曲线，粗略一点说，就是在包含K的任意域中，$f(x, y)=0$ 的全部解的集合。

令 $F(x, y, z)$ 为 d 次齐次多项式，其中 d 为 $f(x, y)$ 的次数，并使$F(x, y, 1)=f(x, y)$，那么 $f(x, y)$ 的亏格 g 为

$$g \geqslant (d-1)(d-2)/2$$

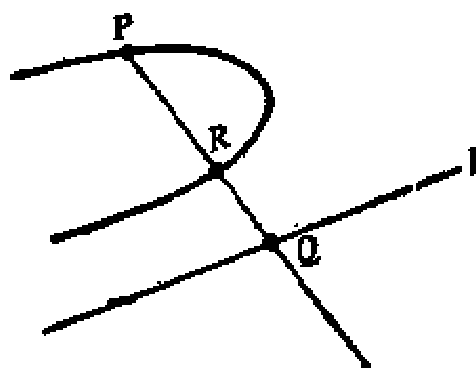
当 $f(x, y)$ 没有奇点时取等号。

费马多项式 x^n+y^n-1没有奇点，其亏格为$(n-1)(n-2)/2$。当 $n\geqslant4$时，费马多项式满足猜想的条件。因此，$x^n+y^n=z^n$ 最多只有有限多个整数解。

为什么猜想中除去了 $f(x, y)$ 的亏格为0或1的情形，即除去了 $f(x, y)$ 的次数 d 小于或等于3的情形呢？我们说明它的理由。

$d=1$ 时，$f(x, y)=ax+by+c$ 显然有无穷多个解。

$d=2$时，$f(x, y)$ 可能没有解，例如 $f(x, y)=x^2+y^2+1$，但是如果它有一个解，那么必定有无穷多个解。我们从几何上来论证这一点。设 P 是 $f(x, y)$解集合中的一点，令 l 表示一条不经过点P的直线（见右图）。对 l 上坐标在域K中的点Q，直线PQ 通常总与解集合交于另一点R。当Q在l上取遍无穷多个K-点时，点R的集合就是 $f(x, y)$ 的K—解的无穷集合。例如把这种方法用于x^2+y^2-1，给出了熟知的参数化解：



$$x=\frac{t^2-1}{t^2+1},\quad y=\frac{2t}{t^2+1}$$

当 $F(X, Y, Z)$ 为三次非奇异（即无奇点）曲线时，其解集合是一个所谓椭圆曲线。我们可用几何方法做出一个解的无穷集。但是，对于次数大于或等于4的非奇异曲线 F，这种几何方法是不存在的。虽然如此，却存在称为阿贝尔簇的高维代数簇。研究这些阿贝尔簇构成了伐尔廷斯证明的核心。

伐尔廷斯在证明莫德尔猜想时，使用了沙伐尔维奇猜想、雅可比簇、高、同源和台特猜想等大量代数几何知识。

莫德尔猜想有着广泛的应用。比如，在伐尔廷斯以前，人们不知道，对于任意的非零整数 a，方程 $y^2=x^3+a$ 在 Q 中只有有限个解。

（四）数理逻辑方法

关于 FLT，逻辑学家关心的是真实性，从给定的公理体系出发，证明定理的可能性和不可判定性问题。我们扼要地解释这些表达式的意义，避免任何技术细节。

FLT涉及通用型的语句，把量词“每一个”放在所有变量的前面：“对于每一个 x，每一个 y，每一个 z，每一个 n：或 $xyz=0$，或 $x^{n+3}+y^{n+3}\neq z^{n+3}$。”把这个语句中的 x，y，z，n 认为非负整数是不言而喻的。如果附有这个说明的语句是真的，那么 FLT 是真的。

这个语句的否定语句是语句：“存在 x，存在 y，存在 z，存在 n，使 $xyz\neq0$ 且 $x^{n+3}+y^{n+3}=z^{n+3}$。”

注 用数理逻辑的符号写出表示 FLT 的命题是：

$(\forall x)(\forall y)(\forall z)(\forall n)\ (xyz=0\ \vee x^{n+3}+y^{n+3}\neq z^{n+3})$

其否定命题是：

$(\exists x)(\exists y)(\exists z)(\exists n)(xyz\neq0\ \wedge x^{n+3}+y^{n+3}=z^{n+3})$

希尔伯特第十问题是：$f(x_1, x_2, \cdots, x_s)$是任给的具有整系数的多项式，给出一个只有有限步运算的方法，来判定方程 $f(x_1,x_2,\cdots,x_s)=0$ 是否有整数解。这个问题的最近解答与 FLT 有关。这在大卫斯、马其雅谢维奇和罗宾逊的1976年论文里有很好的解释。新的思想是转变FLT的证明为检验多项式的方程没有非负的整数解的可能性。

方法是基于以下事实。存在整系数多项式 $P(X, Y, Z, W_1, \cdots, W_k)$，使方程 $Y^Z=X$有

正整数解 $X=a$, $Y=b$, $Z=c$，当且仅当丢番图方程 $P(a, b, c, W_1, \cdots, W_k)=0$ 有正整数解 $W_1=w_1, \cdots, W_k=w_k$.

于是， FLT 是真的当且仅当方程组

$P(A, X+1, N+3, U_1, \cdots, U_k)=0$

$P(B, Y+1, N+3, V_1, \cdots, V_k)=0$

$P(A+B, Z, N+3, W_1, \cdots, W_k)=0$

没有正整数解 a, b, x, y, z, n, $u_1, \cdots, w_k$，其中 A, B, X, Y, Z, N, $U_1, \cdots, U_k$, $V_1, \cdots, V_k$, $W_1, \cdots, W_k$ 是未定元. 考虑多项式 P 的平方，这等价于多项式的方程.

$P^2(A, X+1, N+3, U_1,\cdots,U_k)+P^2(B, Y+1, N+3, V_1, \cdots, V_k)+P^2(A+B, Z, N+3, W_1, \cdots, W_k)=0$

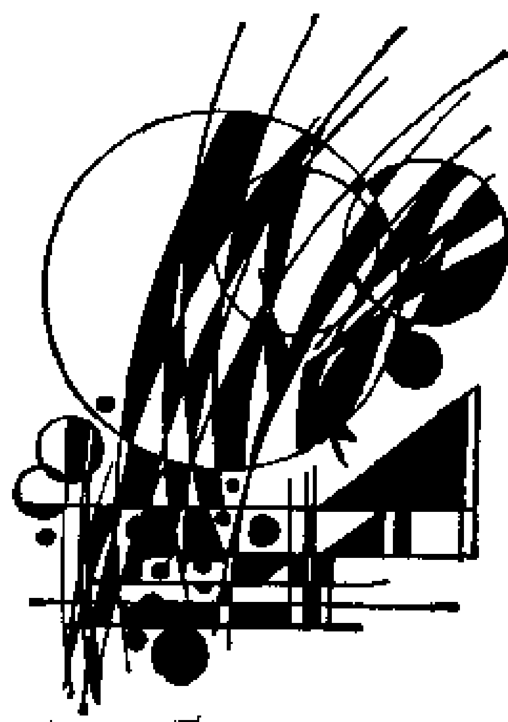
没有正整数解.

现在，明确构造未定元小于12个的多项式P是可能的. 对于更多的未定元有希望吗？

顺便提一下，希尔伯特第十问题已经由苏联青年数学家马其雅谢维奇解决了. 他利用初等数论和数理逻辑方法证明的. 回答是否定的，也就是说不存在这样的方法. （参看本丛书《希尔伯特第十问题》）



六 估 计



在前面几部分里，我们介绍了数学家们在证明 FLT 上所取得的成果。他们的看法主要的如下：

FLT是真的，让我们试图找出证明。对于用复杂的证明取得的每一个进步都是值得做的，尽管它仅处理第一种情形，或仅涉及特定的指数。

由于这个关系，越来越多的复杂方法获得了成功，我们必须承认，仅相对的较小的成功。這些挫折提醒一些数学家开始怀疑 FLT 的真实性。但是，他们的工作在证明定理上是有益的。

我们开始将用初等方法着手估价对于某些给定的指数P的最小正数解的大小。对于第一种情形的一些更精确的估计基于包含 FLT 的标准。

现在，丢番图近似方法和对数的线性型成为攻克问题新的工具，它仍有开拓的必要。

（一）初等估计

方法如下：令 n是某些自然数，$n>2$，并且令 x，y，z 是实数，使

$$0<x<y<z \tag{1}$$

和

$$x^n+y^n=z^n \tag{2}$$

1856年，格鲁耐特证明：

定理1 如果 $0<x<y<z$ 是整数，并且 $x^n+y^n=z^n$，那么 $x>n$。

证明

$$x^n=z^n-y^n=(z-y)(z^{n-1}+z^{n-2}y+\cdots+y^{n-1})>(z-y)ny^{n-1}$$

因此

$$0<z-y<\frac{x^n}{ny^{n-1}}<\frac{x}{n}$$

和

$$y+1\leqslant z<y+\frac{x}{n}$$

于是 $n<x$。□

定理指出，对于 FLT 必须包含大整数的计

算。例如，如果 $n=101$，那么 $x>102$，包含最小如102^{101}大的数。事实上那是相当易懂的，如果没有一些强有力的方法，指出某些可能的解必须是相当大的数。

从上面的证明，得到

$$y<z<y+\frac{x}{n}<y\left(1+\frac{1}{n}\right) \qquad (3)$$

因此 z，y 彼此很近，而 x 的范围必须很小。

另一方面，1969年斐利沙斯特利指出：

$$z<x^2 \qquad (4)$$

得到进一步的估计，采用正实数 r，s，t，r_1，s_1，t_1 是便利的，规定如下：如果$n=p$是奇素数，$0<x<y<z$ 是实数并且 $x^p+y^p=z^p$，令

$$x+y=t^p,\ \frac{x^p+y^p}{x+y}=t_1^p,\ z=tt_1$$

$$z-y=r^p,\frac{z^p-y^p}{z-y}=r_1^p,\ x=rr_1 \qquad (5)$$

$$z-x=s^p,\frac{z^p-x^p}{z-x}=s_1^p,\ y=ss_1$$

这些关系式使我们联想起阿贝尔得到的那些式子（参见第三部分（一））．这些数都是整数不是必然的。然而，如果 x，y，z 都是非零的

整数，并且 $p\nmid xyz$，那么上面的数全是整数。

从（5）式得到

$$x=\frac{r^p-s^p+t^p}{2},y=\frac{-r^p+s^p+t^p}{2},$$

$$z=\frac{r^p+s^p+t^p}{2} \tag{6}$$

和

$$x+y-z=-\frac{r^p+s^p-t^p}{2} \tag{7}$$

显而易见

$$0<r<s<t \tag{8}$$

对于第一种情形更好的界限如下：

定理2 如果 x，y，z 是整数，$p\nmid xyz$ 并且 $x^p+y^p=z^p$，那么 $x>6p^3$。如果 $p\mid xyz$，那么 $x>6p^2$。

探索改进费马方程可能解的下界是众多论文的目标。我们不准备逐个介绍这些改进。

这里，我们介绍依恩柯利的估计，它是现代所知的最好估计。依恩柯利陆续指出（1946）：

$$0<t_1<s_1<r_1 \tag{9}$$

如果 $2\leqslant y$（例如，如果 x，y 是整数），那么 $t<t_1$。　　(10)

从规定这两个不等式是十分明显的。更多的

工作需要指出

$$t_1 > \frac{t^{p-1}}{2} \text{ 和 } t-s > \frac{r}{2p}. \qquad (11)$$

最后，依恩柯利指出（1953）：

定理 3 如果p是一个奇素数，$0<x<y<z$是互素的整数，使 $x^p+y^p=z^p$，并且$p\nmid xyz$，那么

$$x > \left(\frac{2p^3+p}{\log(3p)}\right)^p$$

类似地，依恩柯利得到第二种情形的界限：

定理 4 如果 p是一个奇素数，$0<x<y<z$ 是互素的整数，使 $x^p+y^p=z^p$并且 $p\mid xyz$，那么

$$x > p^{3p-4} \text{ 和 } y > \frac{1}{2}p^{3p-1}.$$

因为对于每一个素指数 $p<3\times10^9$第一种情形是真的，那么在此情形下，x最少有12×10^{10}位数。类似地，在第二种情形下，x 最少有18×10^5位数。

另外有趣的估计由依恩柯利和波奥尔廷得到（1977），它给出下列依据指数 p 对于差$z-x$的下界：

$$z-x > 2^p p^{3p} \qquad (12)$$

（二）土厄、罗思、西格尔和贝克

人们叫做有效方法，是指求某些类不定方程整数解的绝对值的上界。

不能证明 $x^p+y^p=z^p$ 仅有平凡解，一个好的替换方法是指出（对于每一个指数 p）方程最多只有有限个解。

较好地，是决定一个数 $C(p)>0$，使如果 $x^p+y^p+z^p=0$，其中 x，y，z 是非零的互素整数，那么

$$\max\{|x|, |y|, |z|\}<C(p)$$

最后，这个意向更好的可能是决定一个数 $C>0$，使如果 p 是一个素数，并且 $x^p+y^p+z^p=0$，那么

$$\max\{p, |x|, |y|, |z|\}<C$$

无论 C 值或大或小，其结果本质上意味着FLT的解决．余下的工作是对于每一个小于 C 的素数 p 的研究，并且由于估计已经知道（另外的情形尚未发现），解决这个问题出现可能性。

沿着这个方向早期的工作属于土然，以及后来的笛内斯和土然。

1951年，用解析数论的标准方法（特别使用素数定理），土然证明下列结果：

令 $N>1$ 是整数，$v_p(N)$ 表示整数点 (x, y, z) 的个数，使 $(x, y, z)=1$，$x^p+y^p=z^p$（这里 p 是奇素数）并且 $1\leqslant x, y, z\leqslant N$。证明对于指数 p 的 FLT，等于指出对于每一个 $N\geqslant 1$，$v_p(N)=0$。土然的结果距下列结果相差很远：存在一个常数 $C>0$，使其对每一个 N

$$v_p(N)<p(1+3\times 2^{1/p})N^{2/p}$$

在1955年的联合论文中，笛内斯和土然使用初等方法第一次给出上述结果。使用深奥的解析估计，他们得到更好的结果：

$$v_p(N)<C(p)\frac{N^{2/p}}{(\log N)^{2-(2/p)}}$$

他们也猜测

$$v_p(N)<CN^{1/p}$$

或者对于每一个 $e>0$，

$$v_p(N)<C(e)N^{e}$$

在以上不等式中，C，$C(p)$，$C(e)$ 表示正实数。

无论如何土然的猜测不能应用到对于指数 p 费马方程仅有有限个整数解。

丢番图逼近的现代方法基于土厄、罗思、西格尔和更近的贝克的工作，它给出一些希望，新

的结果可以看得见。

按照土厄的思想，罗思证明：

定理1 令 $n\geqslant 3$，

$$F(X,Y)=a_0X^n+a_1X^{n-1}Y+\cdots+a_{n-1}XY^{n-1}+a_nY^n$$

这里 $a_i\in \mathbf{Z}$，$a_0\neq 0$，并且假设 $F(1, X)$ 的根是不同的。令$G(X, Y)\neq 0$的系数在 $\mathbf{Z}$中，总计次数至多为 $n-3$。那么丢番图方程 $F(X,Y)=G(X,Y)$至多有有限个解 $(x, y)\in \mathbf{Z}\times \mathbf{Z}$。

特殊情形 $G(X,Y)=a\in \mathbf{Z}, a\neq 0$，由土厄于1909年证明。特别

定理2 如果 $n\geqslant 3$，a，b，c是整数，a，c 不为零，那么方程 $aX^n+bY^n=c$ 至多有有限个整数解。

取 $a=1$，$b=1$，$c=z^n$，当 n 为奇数时，对于每一个 $z\neq 0$至多存在有限多个整数 x，y 使 $x^n+y^n=z^n$。

还有两个结果如下：

西格尔的定理指出：

定理3 如果由 $f(x, y)=0$确定的曲线不是有理曲线（换句话说它的亏格大于0），那么仅存在有限多整数对 (x, y)使得 $f(x, y)=0$。

1976年，泰做曼和辛宰尔证明：

定理4 如果 $m\geqslant 2$，$n\geqslant 2$并且$\max\{m,n\}\geqslant 3$，$f(X)\in \mathbf{Z}[X]$的次数为 n并且有单根，$a\neq 0$是整数，那么方程 $f(X)=aY^m$ 至多有有限个整数解。

贝克的更现代方法涉及对数线性型的有效正的下界。1964年贝克考虑线性型

$$\Lambda=b_1\log\alpha_1+b_2\log\alpha_2+\cdots+b_n\log\alpha_n \quad (1)$$

这里 $n\geqslant 1$，α_1，α_2，…，α_n 是一些代数整数，b_1，b_2，…，b_n 是一些有理整数，log 表示对数函数主测定 (principal determination)。

令 d 是 Q 的扩域 $Q(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 的次数。对于每一个 α_i，令 $H(\alpha_i)$ 是它的高，规定如下：令 $f(X)=c_0X^m+c_1X^{m-1}+\cdots+c_m$ 仅是整系数多项式，使得 $(c_0, c_1, \cdots, c_m)=1$ 和 $f(\alpha_i)=0$，那么 $H(\alpha_i)=\max_{0\leqslant i\leqslant m}\{|c_i|\}$。

令 $A_i=\max\{4, H(\alpha_i)\}$，对于 $i=1, 2, \cdots, n$，把 A_i 编号，使 $A_1\leqslant A_2\leqslant\cdots\leqslant A_n$，并且令 $B=\max_{1\leqslant i\leqslant n}\{|b_i|, 4\}$。

假设 $\Lambda\neq 0$。贝克指出（1977），$|\Lambda|$方便的下界是

$$|\Lambda|>\exp\{-2^{\gamma_1 n+\gamma_0}n^{\gamma_2 n}d^{\gamma_3 n+\gamma_4}(\log B)(\log A_1)\cdots(\log A_n)(\log\log A_{n-1})\} \quad (2)$$

这里 γ_0，γ_1，γ_2，γ_3，γ_4 是正实数，可以有效

地计算，并且不依赖于n，a_i，b_i。

例如，贝克指出：

$$\gamma_0=0,\ \gamma_1=800,\ \gamma_2=200,\ \gamma_3=200,\ \gamma_4=0 \quad (3)$$

这时，

$$|\Lambda|>\exp\{-(16nd)^{200n}(\log B)(\log A_1)\cdots(\log A_n)(\log\log A_{n-1})\} \quad (4)$$

波奥尔廷和罗克斯顿于1977年给出下列更好的常数值：

$$\gamma_0=47,\gamma_1=61,\gamma_2=10,\gamma_3=10,\gamma_4=10 \quad (5)$$

贝克方法的主要应用是证明一定型的丢番图方程的解的有效界限。对于莫德尔方程$Y^2=X^3+k$ ($k\neq0$)，贝克在1968年证明：如果x,y是整数并且$y^2=x^3+k$，那么

$$\max\{|x|,\ |y|\}<\exp\{(10^{10}|k|^{10^4}\} \quad (6)$$

贝克方法最显著的应用由泰德曼于1976年得到，它关系到卡塔兰方程

$$X^m-Y^n=1$$

其中m，n是大于或等于2的整数。1844年卡塔兰猜想，如果x，y是自然数并且$x^m-y^n=1$，那么$x=3$，$y=2$，$m=2$，$n=3$。

虽然许多数学家在这方面做出努力，但这个猜想至今没有被普遍地证明。

使用贝克的方法，可以证明：如果m，$n \geqslant 2$给定，x, y 是自然数，使 $x^m - y^n = 1$，那么

$$\max\{x, y\} < \exp \exp \{(5n)^{10} m^{10^{m^3}}\} \quad (7)$$

泰笛曼稍微改进贝克关于对数线性型的下界，证明：存在一个可有效计算的数 $C \geqslant 3$，使得如果 x，y，m，n是自然数，m，$n \geqslant 2$，并且$x^m - y^n = 1$，那么

$$\max\{x, y, m, n\} < C$$

1975年，兰哥文证明：

$$C \leqslant \exp \exp \exp \exp 730$$

（三）新方法的应用

上面我们介绍了一些有效方法，同时给出它们的一些应用。这里，我们将着重介绍它们在解决 FLT 上的几个应用。

第一个结果属于依恩柯利（1946）：

定理1　令$n \geqslant 3$，M是一个正整数。

a．仅存在有限多整数组（x，y，z）使$0 < x < y < z$，$x^n + y^n = z^n$ 和 $y - x < M$。

b．同上，$z - y < M$。

在两种情形下，

$$z<\exp\ \exp\{(5n)^{10}(n^{10n}A)^{n^2}\} \quad (1)$$

其中

$$A=\max_{1\leq i\leq n}\left\{\binom{n}{i}M^i\right\}$$

我们还要指出，对于第一种情形用完全初等的方法，依恩柯利得到更好的界限。就是，如果 $x^p+y^p=z^p$，$0<x<y<z$，$p\nmid xyz$，并且 $y-x<M$，那么

$$z<\frac{\sqrt[p]{2}M^{p/(p-1)}}{\sqrt[p]{2}-1}$$

如果 $z-y<M$，那么

$$z<\frac{\sqrt[p]{2}M^p}{\sqrt[p]{2}-1}$$

这说明一个事实，如果用初等方法得到界限是可能的，结果证明它比贝克方法得到的界限要好得多。

可以证明，如果 $n>2$，$0<x<y<z$ 是互素的整数，使 $x^n+y^n=z^n$，那么 y，z 不是素数的幂。如果 x 是素数的幂，那么 $n=p$ 是奇素数，并且 $z=y+1$。

依恩柯利指出（1946）：

定理2 在上述假设下，并且 $n=p$ 不整除 xyz，那么 x 不是一个素数幂。

对于第一种情形没有什么比初等方法更有用。然而，对于第二种情形，用有效方法，依恩柯利仅取得部分成果：

定理3 令 $p\geqslant 3$. 那么至多存在有限多个互素的整数组 (x, y, z)，使 $0<x<y<z$, $x^p+y^p=z^p$ 和 x 是一个素数幂。对于每一个这样的数组，$z=y+1$, $p\mid y(y+1)$和

$$y<\exp\ \exp\{2^p(p-1)^{10(p-1)}\}^{(p-1)^2}$$

$$<\exp\ \exp(2p^{10})^{p^2}$$

在上述情形下，鉴于瓦格斯塔夫的计算，$p>125000$.对于 y用依恩柯利在第六部分（一）里给出定理4，得

$$\frac{1}{2}p^{3p-1}<y<\exp\ \exp(2p^{10})^{p^2}$$

由于上述间隔如此之大，使其得不到任何实际上的结果。

作为一个定理的特殊情形，我们有

定理4 令$M>0$ 是给定的实数，p 是奇素数和 $0<x<y<z$ 是互素的整数，使 $x^p+y^p=z^p$. 如果下列条件

$$y-x<M(z-x)^{1-(1/\sqrt{p})}$$

被满足，那么存在依赖M的正实数C，可以有效计算，使得

$p<C$

一个更简单和更有启发性的结论如下：

定理 5 令$\varepsilon>0$是实数，p是奇素数，$0<x<y<z$是互素的整数，使$x^p+y^p=z^p$和$y-x<2^{(1-\varepsilon)p}$。那么存在一个可直接计算的常数C，使得$p<C$。

事实上，定理 5 中的指数不必要是素数，这就构成一个重要的一般性定理：

定理 6 给定$M>0$，存在数$C>0$（依赖M可直接计算），使得如果$n\geqslant3$是整数，x,y,z是互素的整数，$x^n+y^n=z^n$，其中$0<x<y<z$，那么：若$2<z-y<M$或$y-x<M$，则x，y，z都小于C。

依恩柯利和波奥尔廷证明下列相当技术的结果：

定理 7 令p是奇素数，l_1，l_2，…，l_m（其中$m\geqslant0$）是不同的素数，$l_i<p$；令w_1，w_2，…，w_m是自然数。如果x，y，z是互素的整数，使$0<x<y<z$，$x^p+y^p=z^p$并且$\prod_{i=1}^{m}l_i^{w_i}$整除$y-x$，那么

$$\frac{y-x}{\prod_{i=1}^{m} l_i^{v_i}} > (z-x)^{1-\{L(\log p)^3/(p-1)\}}$$

这里 $L=B(1+l_1+\cdots+l_m)$，其中

$z-x=b^p$，$z-y=p^{p-1}a^p$ 当 $p \mid x$，

$z-x=p^{p-1}b^p$，$z-y=a^p$ 当 $p \mid y$，

$z-x=b^p$，$z-y=a^p$ 当 $p \nmid xy$。

定理 8 给定素数 l_1，l_2，…，l_m 和整数 $M_0>0$，存在可直接计算的数 $C>0$，使得如果 x，y，z 是互素的整数，$0<x<y<z$，$x^p+y^p=z^p$，并且如果对于每一个非负的整数 w_1，w_2，…，w_m，有

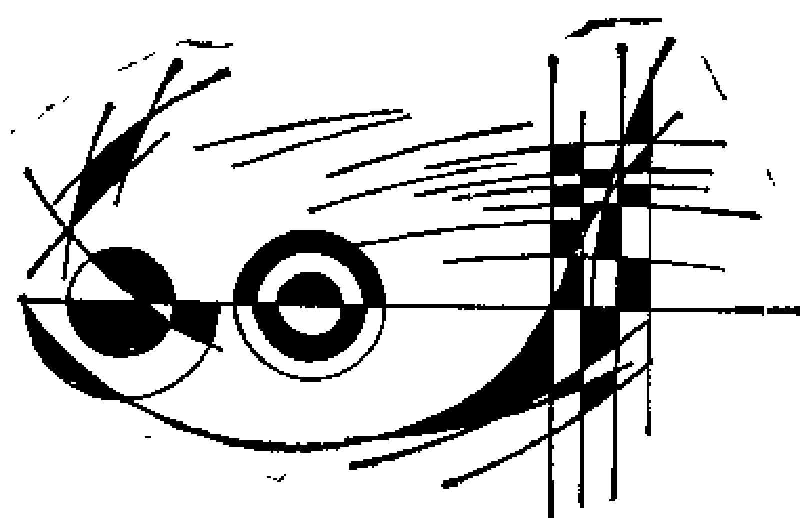
$$y-x<M_0 l_1^{w_1}\cdots l_m^{w_m}(z-x)^{1-(1/\sqrt{p})}$$

那么 $p<C$。

在这些努力中，共同的思想是寻求一个可有效计算的数，做为指数的界限。如何没有任何假定可以做到，这就意味着至少在理论上FLT的解决。但是，到目前为止关于指数的界限仅在可能解的性质的各种或多或少技术假设下得到的。



七　费马猜想的推广



前面几部分里，我们介绍了 FLT 的历史情况以及一些现代成果。费马方程 $x^p+y^p=z^p$ 是三元齐次方程。本部分里，将要介绍由于费马方程的元数、系数和指数的变化而产生的丰富内容。

(一) $x^3+y^3+z^3=w^3$

我们已经知道，方程

$$x^3+y^3=z^3$$

没有正整数解。但是，方程

$$x^3+y^3+z^3=w^3$$

或

$$x^3+y^3+z^3+t^3=0 \qquad (1)$$

却有无穷多整数解。

事实上，设 a，b，c，d 和a_1，b_1,c_1,d_1 是（1）的两个解。我们适当选择k 的值，使

$$a+ka_1,\ b+kb_1,\ c+kc_1,\ d+kd_1 \qquad (2)$$

也是（1）的一个解。为此，下列等式成立：

$$(a+ka_1)^3+(b+kb_1)^3+(c+kc_1)^3+(d+kd_1)^3=0$$

去括号，再根据假设可以得到

$$3k[a^2a_1+b^2b_1+c^2c_1+d^2d_1)+k(aa_1^2+bb_1^2+cc_1^2+dd_1^2)]=0$$

从而，若 $k=0$,得一解为 a，b，c，d，不取；若 $k\neq0$,由上式左边第二个因式得

$$k=-\frac{a^2a_1+b^2b_1+c^2c_1+d^2d_1}{aa_1^2+bb_1^2+cc_1^2+dd_1^2} \qquad (3)$$

如果k取（3）式的值，那么就可以从（1）的两个解求出第三个解来。现在的问题是，能否找出（1）的两个整数解来。回答是肯定的。例如，

$$a=3,\ b=4,\ c=5,\ d=-6;$$

$$a_1=r,\ b_1=-r_1,\ c_1=s,\ d_1=-s.$$

这样一来，由（3）给出的k 为

$$k=\frac{7r+11s}{7r^2-s^2} \qquad (4)$$

从而，得到（1）的解为

$$\begin{cases} x=28r^2+11rs-3s^2 \\ y=21r^2-11rs-4s^2 \\ z=35r^2+7rs+6s^2 \\ t=-42r^2-7rs-5s^2 \end{cases} \quad (5)$$

若给出（5）中的 r 和 s 一些整数值，则可得到（1）的整数解。如果得到的解有公因数，可把公因数约去。例如，

$r=1$，$s=1$时，$6^3+1^3+8^3+(-9)^3=0$；

$r=1$，$s=2$时，$38^3+73^3+(-17)^3+(-76)^3=0$；

$r=1$，$s=-1$时，$7^3+14^3+17^3+(-20)^3=0$；

$r=2$，$s=-1$时，$29^3+34^3+44^3+(-53)^3=0$；

…… …… …… …… …… ……

如果把开始解的四个数调换一下位置，用同样的方法，能够得到一个全新的解。例如，取 $a=3$，$b=5$，$c=4$，$d=-6$，a_1，b_1，c_1，d_1 不变，得到

$$\begin{cases} x=20r^2+10rs-3s^2 \\ y=12r^2-10rs-5s^2 \\ z=16r^2+8rs+6s^2 \\ t=-24r^2-8rs-4s^2 \end{cases} \quad (6)$$

从（6）我们又可以得到（1）的一些解。

例如，

$r=1$，$s=3$时，$23^3+94^3+(-63)^3+(-84)^3=0$；

$r=2,s=1$时，$23^3+97^3+83^3+(-116)^3=0$；

$r=1,s=-3$时，$3^3+36^3+37^3+(-46)^3=0$；

… … … … … …

我们还可以用上面得到的任意两个解为开始解，再求出新的解来。这样一来，用上述方法可求得（1）的无穷多个整数解。

方程（1）的整数解还可以从下列一些恒等式得出：

$$(3a^2+5ab-5b^2)^3+(4a^2-4ab+6b^2)^3+(5a^2-5ab-3b^2)^3=(6a^2-4ab+4b^2)^3 \quad (7)$$

其中a，b取整数。

$$(m^2+16m-21)^3+(16m-m^2+21)^3+(2m^2-4m+42)^3=(2m^2+4m+42)^3 \quad (8)$$

其中m取整数。

$$(k^2-l)^3+(-k^2-m)^3=(km-1)^3+(-kl+1)^3 \quad (9)$$

这里 $k=a^2+3b^2$，$l=a-3b$，$m=a+3b$，a，b取整数。

$$(3u^2v+2uv^2+v^3)^3+(uv^2)^3+(3u^3+3u^2v+2uv^2)^3=(3u^3+3u^2v+2uv^2+v^3)^3 \quad (10)$$

这里 u, v 取整数。

值得指出的是，迄今为止还没有找到（1）的全部整数解公式。但是，欧拉一比耐特找到了（1）的全部有理数解公式：

$$\begin{cases} x=\frac{1}{2}(W+X+Y+Z) \\ y=\frac{1}{2}(W+X-Y-Z) \\ z=\frac{1}{2}(W-X+Y-Z) \\ t=\frac{1}{2}(W-X-Y+Z) \end{cases} \tag{11}$$

这里，

$W=-6\rho abc$, $X=\rho a\ (a^2+3b^2+3c^2)$,

$Y=\rho b(a^2+3b^2+9c^2)$, $Z=3\rho c(a^2+b^2+3c^2)$,

其中 $(a, b, c)=1$，且 ρ为有理数。

关于多未知数的三次齐次方程，我们给出下列一些等式：

$3^3+4^3+5^3+8^3+10^3=12^3=6^3+8^3+10^3$;

$1^3+3^3+4^3+5^3+8^3=9^3=1^3+6^3+8^3$;

$1^3+5^3+6^3+7^3+8^3+10^3=13^3=5^3+7^3+9^3+10^3$;

$2^3+3^3+5^3+8^3+9^3+10^3=14^3$

$11^3+12^3+13^3+14^3=20^3$;

$$230^3+243^3+256^3+269^3+282^3=440^3;$$

$$435^3+506^3+577^3+648^3+719^3+790^3=1155^3.$$

我们还可以给出几十个、甚至上千个数的立方的等式。例如，

$$6^3+7^3+8^3+\cdots+68^3+69^3=180^3;$$

$$1134^3+1135^3+1136^3+\cdots+2132^3+2133^3=16830^3.$$

（二） $x^3+y^3+z^3=n$

方程

$$x^3+y^3+z^3=1 \qquad (1)$$

有无穷多个整数解。它们可从下列恒等式得到：

$$(9n^4)^3+(1-9n^3)^3+(3n-9n^4)^3=1 \qquad (2)$$

其中 n 为自然数。

方程

$$x^3+y^3+z^3=2 \qquad (3)$$

有无穷多个整数解。它们可从下列恒等式得到：

$$(1+6n^3)^3+(1-6n^3)^3+(-6n^2)^3=2 \qquad (4)$$

其中 n为自然数。

方程

$$x^3+y^3+z^3=3 \qquad (5)$$

除了下列四个解：

1，1，1；4，4，－5；4，－5，4；－5，4，4．

还有另外的解吗？这是一个非常困难的问题。

我们还不知道方程

$$x^3+y^3+z^3=30 \qquad (6)$$

是否有整数解。

一般地，方程

$$x^3+y^3+z^3=n \qquad (7)$$

对于某些整数 n，它可以有无穷多个整数解。例如，$n=a^3$ 时，（7）有整数解

$$x=t,\ y=-t,\ z=a \qquad (8)$$

和

$$x=9at^4,\ y=3at-9at^4,\ z=a-9at^3 \qquad (9)$$

其中 a，t 为整数。

当 $n=2a^3$ 时，（7）有整数解

$$x=a(1+6t^3),\ y=a(1-6t^3),\ z=-6at^2 \qquad (10)$$

其中 a，b 为整数。

但是，对于某些整数 n，（7）也可能没有整数解．例如，$n\equiv\pm4 \pmod 9$ 时，（7）没有整数解。

事实上，因为 $x^3\equiv\pm1,\ 0 \pmod 9$，$y^3\equiv$

± 1，0 (mod 9)，$z^3 \equiv \pm 1$，0 (mod 9)，所以 $x^3+y^3+z^3 \not\equiv \pm 4$ (mod 9)。因此（7）没有整数解。

最后，我们给出一个更一般的结果：

方程

$$a(x^3+y^3)+bz^3=bc^3 \tag{11}$$

其中 a，b，c 是整数，$abc \neq 0$，除了平凡解 $x+y=0$，$z=c$ 外，还有无穷多个整数解：

$$x=\frac{u+v}{2}, y=\frac{u-v}{2}, z=c+tu \tag{12}$$

其中 $u \equiv v$ (mod 2)。当 $u=0$ 时，(12) 便是平凡解。

此果把（7）的变量增至四个，我们有：

定理 如果方程

$$x^3+y^3+z^3+w^3=n \tag{13}$$

有一个整数解 $x=a$，$y=b$，$z=c$，$w=d$，使 $-(a+b)(c+d)>0$ 不是平方数，且 $a \neq b$ 或 $c \neq d$，那么 (13) 有无穷多个整数解。

推论 方程

$$x^3+y^3+z^3+w^3=1 \tag{14}$$

$$x^3+y^3+z^3+w^3=2 \tag{15}$$

$$x^3+y^3+z^3+w^3=3 \tag{16}$$

都有无穷多个整数解。

证明 方程（14）有整数解 $x=1$，$y=2$，$z=0$，$w=-2$，$-(a+b)(c+d)=6>0$，且不是平方数．根据定理（14）有无穷多个整数解．

同样，方程（15）有整数解 $x=1$，$y=2$，$z=-2$，$w=1$，（16）有整数解 $x=y=4$，$z=-5$，$w=0$，并且它们都满足定理的条件，故（15）和（16）都有无穷多个整数解．□

关于方程（13）有一个著名的猜想：对于每一个整数 n，方程（13）有整数解．

已经证明，对于 $n\not\equiv\pm4 \pmod 9$ 任何整数 n，猜想成立．柯召教授证明在 $|n|\leqslant100$ 时猜想成立．目前，猜想仅在 $n<1000$时被证明是对的．

（三）三次的方程

我们首先讨论方程

$$x^3+y^3=kz^3 \tag{1}$$

的整数解情况，其中 k是给定的正整数．

当 $k=1$ 时，（1）变为熟知的 $n=3$ 时 FLT，它没有非零的整数解．

当 $k=2$ 时，方程（1）有非零的整数解，

且仅为 $x=y=z$，z 为任意的非零整数。由此可以得到，对于 $k=2n^3$，其中 n 为自然数，方程（1）有非零的整数解，且仅为 $x=y=nz$，z 为任意的非零整数。这样一来，进一步我们能够假设 k 不为 $k=2n^3$ 型的正整数，其中 n 为自然数。

对于自然数 k，$2\leqslant k\leqslant 10$，方程（1）有非零的整数解 x，y，z，仅当 $k=6$（例如，$x=17$，$y=37$，$z=21$），$k=7$（例如，$x=-17$，$y=73$，$z=38$）和 $k=9$（例如 $x=2$，$y=z=1$）。

显然，如果（1）有一个非零的整数解，那么它有无穷多个整数解。但是，能够证明，如果 k 不为 $2n^3$ 型整数，n 为自然数，那么从（1）的每一个非零的整数解 x，y，z，能够得到另外的非零整数解 x_1，y_1，z_1，并且 x_1，y_1，z_1 与数 x，y，z 不成比例。这一点可从下列恒等式得出：

$$[x(x^3+2y^3)]^3+[-y(2x^3+y^3)]^3 = (x^3+y^3)(x^3-y^3)^3 \tag{2}$$

如果取

$$x_1=x(x^3+2y^3),\quad y_1=-y(2x^3+y^3),\quad z_1=z(x^3-y^3) \tag{3}$$

那么根据（1）和（3），有

$$x_1^3 + y_1^3 = kz_1^3 \tag{4}$$

并且 x_1, y_1, z_1 不为零。事实上，如果 $x_1=0$，考虑 $x\neq0$，从（3）可知 $x^3+2y^3=0$，或 $x^3=-2y^3$，由于 $y\neq0$，此式不成立。同样可以证明，$y_1=0$ 也不可能。最后，如果 $z_1=0$，考虑 $z\neq0$，从（3）可知 $x^3=y^3$。此时（1）变为 $2x^3=kz^3$。容易看出 k 必为 $k=2n^3$，其中 n 为自然数，而这与假设矛盾。此外，容易看出 x_1, y_1, z_1 与 x, y, z 不成比例。

例如，从方程 $x^3+y^3=9z^3$ 的整数解 $x=2$, $y=1$, $z=1$，得到新的解 $x_1=20$, $y_1=-17$, $z_1=7$。

容易证明，方程（1）有非零的整数解的充分且必要条件是 $k=ab(a+b)c^{-3}$，其中 a, b, c 是非零的整数。

证明　条件是必要的。如果非零的整数 x, y, z 适合方程（1），那么取 $a=x^3$, $b=y^3$, $c=xyz$，得到非零的整数，而且根据（1）有 $ab(a+b)=kc^3$。

条件的充分性可从恒等式

$$(a^3-b^3+6a^2b+3ab^2)^3+(b^3-a^3+6ab^2+3a^2b)^3=ab(a+b)3^3(a^2+ab+b^2)^3 \tag{5}$$

得到证明。如果 $a^3-b^3+6a^2b+3ab^2=0$，用 d 表

示 a 与 b 的最大公因数，则 $a=da_1$，$b=db_1$，其中 a_1，b_1 是非零的整数，并且互素。这时，得到 $a_1^3-b_1^3+6a_1^2b_1+3a_1b_1^2=0$。因此，$a_1^3$ 被 b_1 整除，b_1^3 被 a_1 整除，并考虑 a_1 与 b_1 互素，必有 $a_1=\pm1$，$b_1=\pm1$，因而 $a=\pm b$。$a=-b$ 时，则 $k=ab(a+b)c^{-3}=0$，与 k 是正整数的假设矛盾。$a=b$ 时，则 $k=2b^3c^{-3}$，因此容易得出 $k=2n^3$，其中 n 是自然数。于是（1）存在正整数解 $x=y=n$，$z=1$。类似可证 $b^3-a^3+6ab^2+3a^2b=0$的情形。最后 $a^2+ab+b^2=0$是不可能的，因为 $4(a^2+ab+b^2)=(2a+b)^2+3b^2\geqslant 3b^2>0$，其中 $b\neq0$。

因此，数组

$$\left\{\begin{aligned}x&=\frac{1}{c}(a^3-b^3+6a^2b+3ab^2)\\y&=\frac{1}{c}(b^3-a^3+6ab^2+3a^2b)\\z&=3(a^2+ab+b^2)\end{aligned}\right.\qquad(6)$$

全不为零，根据恒等式 $k=ab(a+b)c^{-3}$，它们适合方程（1）。充分性得证。□

其次，我们给出几个三次方程的整数解情况。

方程

$$x^3+y^3=z^2 \tag{7}$$

有无穷多个整数解 x，y，z.因为$1^3+2^3=3^2$，并且由于方程（7）的性质，如果 x，y，z 适合方程（7），那么对整数 d，有

$$(xd^2)^3+(yd^2)^3=(zd^3)^2$$

所以（7）有无穷多个整数解。

还可以借助于恒等式

$$(x^3+4y^3)^3-(3x^2y)^3=(x^3+y^3)(x^3-8y^3)^2 \tag{8}$$

从方程（7）给定的解得到另外的解。

如果我们取

$$x_1=x^3+4y^3,\quad y_1=-3x^2y,\quad z_1=(x^3-8y^3)z$$

那么将有

$$x_1^3+y_1^3=z_1^2$$

例如，从方程（7）的解$x=1,y=2,z=3$，可以得到解

$$33^3+(-6)^3=(-3^3\cdot7)^2$$

方程

$$x^3+(x+1)^3=y^2 \tag{9}$$

仅有两个整数解：$x=0$，$y=1$；$x=1,y=3$。

方程

$$x^3+y^3+z^3=t^2 \tag{10}$$

有无穷多个整数解 x，y，z，t.它们可从下列恒

等式得到：

$$[u(u^3+2)]^3+(2u^3+1)^3+(3u^2)^3$$
$$=(u^6+7u^3+1)^2 \qquad (11)$$

其中 u取整数。

例如，$u=2$ 时，得到

$$20^3+17^3+12^3=121^2=11^4$$

从此，我们也得知，方程

$$x^3+y^3+z^3=w^4 \qquad (12)$$

也有整数解。

从（11）式我们还可以得到一般等式：

$$[u(u^3+2v^3)]^3+[v(2u^3+v^3)]^3+(3u^2v^2)^3$$
$$=(u^6+7u^3v^3+v^6)^2 \qquad (13)$$

其中 u，v 为整数，$v\neq 0$。

事实上，把（11）式中的u 用$\dfrac{u}{v}$代替，然后等式两边同乘以 v^{12}，便可得到（13）。例如，取 $u=5$，$v=2$，则

$$705^3+516^3+300^3=22689^2$$

容易证明，方程组

$$\begin{cases} x+y+z=t \\ x^2+y^2+z^2=t^2 \\ x^3+y^3+z^3=t^3 \end{cases} \qquad (14)$$

只有平凡解。

证明 从（14）容易得出

$$xy+yz+zx=0$$

$$(x+y)(y+z)(z+x)=0$$

于是，$x+y$，$y+z$，$z+x$ 中至少有一个为零。例如，$x+y=0$，即 $x=-y$，由上面的第一式，得 $xy=0$，因而 $x=y=0$。由此可以断言，x，y，z 中必有两个为零，其余一个等于 t，t 为任意的整数。因此，方程组（14）除了上述平凡解外，没有其他的整数解。□

（四）四次的方程

这里我们将介绍几个类型的四次方程的整数解情况，它们都是来源于四次的费马方程。

1．$\Sigma x_i^4=y^4$

我们已经证明，方程

$$x^4+y^4=z^4$$

没有正整数解。欧拉曾猜测，方程

$$x^4+y^4+z^4=t^4 \tag{1}$$

没有正整数解。1945年，约尔得证明，对于 $t<10^4$（1）没有正整数解。

但是，方程

$$x^4+y^4+z^4+t^4=w^4 \qquad (2)$$

却有整数解。

哈特给出：

$$4^4+6^4+8^4+9^4+14^4=15^4 \qquad (3)$$

马丁提出等式

$$1^4+(2m)^4+96(m^2)^4+(4m^3)^4+(4m^4)^4$$
$$=(1+4m^4)^4 \qquad (4)$$

但$96=3^4+2^4-1^4$.于是新的左边有六个正的四次幂和一项〔$-(m^2)^4$〕。对于 $m=2$，消去$(2m)^4$，我们得到

$$1^4+8^4+12^4+32^4+64^4=65^4$$

对于 $m=3$，则

$$A+108^4+324^4=325^4$$

这里$A=1^4+6^4+18^4+27^4-9^4=28^4+10^4+8^4+7^4$
$=26^4+20^4+10^4+8^4+3^4$.

法奎姆波古给出等式

$$(4x^4+y^4)^4=(4x^4-y^4)^4+(4x^3y)^4+(4x^3y)^4+(2xy^3)^4+(2xy^3)^4 \qquad (5)$$

从上面的讨论可以看出，方程

$$\sum_{i=1}^{s} x_i^4=y^4$$

其中 $n=4$，5，6，7，都有整数解。

2. $x^4+y^4=z^4+t^4$

方程

$$x^4+y^4=z^4+t^4 \tag{6}$$

存在不同的正整数解 x，y，z，t.例如，

$$103^4+542^4=359^4+514^4$$

$$1203^4+76^4=1176^4+653^4$$

欧拉研究过（6）型方程，给出整数解：

$$x=2219449,\ y=-555617,$$

$$z=1584749,\ t=2061283.$$

后来又给出两个正整数解：

$$158^4+59^4=133^4+134^4$$

$$2379^4+27^4=729^4+577^4$$

数学家们陆续又给出：

$$239^4+7^4=227^4+157^4$$

$$292^4+193^4=256^4+257^4$$

3. $\Sigma x_i^4=\Sigma y_i^4$

马丁给出：

$$1^4+2^4+9^4=3^4+7^4+8^4;$$

$$1^4+9^4+10^4=5^4+6^4+11^4;$$

$$1^4+11^4+12^4=4^4+9^4+13^4;$$

$$1^4+5^4+8^4+10^4=3^4+11^4.$$

另一些数学家给出：

$$8^4+9^4+17^4=3^4+13^4+16^4;$$

$$7^4+28^4=3^4+20^4+26^4;$$

$$51^4+76^4=5^4+42^4+78^4.$$

4. $\Sigma x_i^4=ky^2$

从方程

$$x^4\pm y^4=z^2$$

没有正整数解，可得方程

$$x^4+y^4=2z^2 \tag{7}$$

除了 $y=x$，$z=x^2$，没有另外的正整数解，其中 x 是任意的正整数。

事实上，如果 $y\neq x$，那么 $|x^2-y^2|>0$，根据（7），有

$$(x^2+y^2)^4-(x^2-y^2)^4=(4xyz)^2.$$

这与 $x^4-y^4=z^2$ 没有正整数解矛盾。

容易证明，方程

$$x^4+y^4=3z^2 \tag{8}$$

没有正整数解 x，y，z。

方程

$$x^4+y^4=4z^2 \tag{9}$$

即

$$x^4+y^4=(2z)^2$$

没有正整数解。这可直接从 $X^4+Y^4=Z^2$ 没有正整数解得出。

容易证明，方程

$$x^4+y^4=5z^2 \tag{10}$$

没有正整数解。

事实上，可以假设（10）中的 x，y 互素，因而它们不能同时被 5 整除。因为正整数的四次幂被 5 除时的余数为 0 或 1，所以（10）的左边除以 5 时的余数为 1 或 2，而右端除以 5 的余数为 0。故

$$x^4+y^4 \not\equiv 5z^2 \pmod 5$$

因此（10）没有正整数解。

瑞阿利斯指出，方程

$$x^4+y^4+t^4=2z^2 \tag{11}$$

有整数解，如果

$$x=2057\alpha^3-2541\alpha^2\beta+2787\alpha\beta^2-391\beta^3$$

$$y=391\alpha^3-2787\alpha^2\beta+2541\alpha\beta^2-2057\beta^3$$

$$t=(2\alpha+2\beta)(391\alpha^2-730\alpha\beta+391\beta^2)$$

其中 α，β 取整数。

例如，$\alpha=1$，$\beta=0$ 或 1 时，得

$$46^4+121^4+23^4=2\times 10467^2$$

$$26^4+239^4+239^4=2\times 57123^2$$

从等式

$$(4at)^4+(3a^2+2at-t^2)^4+(3a^2-2at-t^2)^4$$
$$+(6a^2+2t^2)^4=2[3(3a^2+t^2)^2]^2 \qquad (12)$$

令 $a=1$, $t=2$,得到

$$3^4+5^4+8^4+14^4=2\times147^2$$

5. $x^4+ky^4=z^2$

定理 如果方程

$$x^4+ky^4=z^2 \qquad (13)$$

其中 k是给定的偶数，有一个整数解 x, y, z, 并且 $(x, ky)=1$,那么它有一个新的解 x_1, y_1, z_1, 并且 $(x_1, ky_1)=1$. 从而它有无穷多个整数解.

证明 假设（13）有正整数解 x, y, z, 且 $(x, ky)=1$. 容易求出

$$(x^4-ky^4)^2+k(2xyz)^4=(z^4+4kx^4y^4)^2 \qquad (14)$$

我们取

$$x_1=|x^4-ky^4|, y_1=2xyz, z_1=|z^4+4kx^4y^4| \qquad (15)$$

进一步讨论可知，x_1, y_1, z_1 是正整数，并且 $(x_1, ky_1)=1$,适合方程（13).

因此，从(13)的每一个正整数解 x, y, z, 其中 $(x, ky)=1$,根据(14)和（15）得到一个新

的正整数解 x_1, y_1, z_1,其中 $(x_1, ky_1)=1$,并且 $y_1>y$. 由此得知,这样的解有无穷多个。

特别,我们取 $k=8$.方程

$$x^4+8y^4=z^2 \tag{16}$$

显然有解 $x=y=1$, $z=3$,其中 $(x, 8y)=1$.

从解 $x=y=1$, $z=3$,根据(15)得到新的解 $x_1=7$, $y_1=6$, $z_1=113$,进一步可得 $x_2=7967$, $y_2=9492$, $z_2=262621633$, ……但方程(16)有另外的解,例如 $x=239$, $y=13$, $z=57123=239^2+2$. 再用上面指出的方法,又可得到另外无穷多个正整数解.

现在取$k=-2$. 方程

$$x^4-2y^4=z^2 \tag{17}$$

有解 $x=3$, $y=2$, $z=7$,且 $(x, ky)=(3, -4)=1$. 从所给的解,根据公式(15)得到新的解, $x_1=113$, $y_1=84$, $z_1=7967$, 等.

这里还要指出,如果

$$x^4-2y^4=\pm z^2 \tag{18}$$

那么

$$z^4+8(xy)^4=(x^4-2y^4)^2+8x^4y^4$$
$$=(x^4+2y^4)^2$$

因此,从(18)的每一个解,可以得到(16)的一个解. 例如,从(17)的解 $x=3$, $y=2$,

$z=7$，可得到（16）的解（7，6，13）。

另一方面，容易证明，从方程（16）的每一个解，可以得到方程（17）的一个解。这点可从下列恒等式直接作出结论：

$$(x^4+8y^4)^2-2(2xy)^4=(x^4-8y^4)^2$$

因此，如果 $x^4+8y^4=z^2$，那么取 $u=z$，$v=2xy$，$w=|x^4-8y^4|$，有$u^4-2v^4=w^2$。例如，从方程（16）的解 $x=7$，$y=6$，$z=113$，得到 $u^4-2v^4=w^2$ 的解 $u=113$，$v=84$，$w=7967$。

困难证明，从方程（16）的解，依据

$$\begin{cases} u=|zx\mp 2x^2y\mp 8y^3| \\ v=|zx\mp 4x^2y\pm 8y^3| \\ w=|48zxy^3\pm x^6\mp 24x^4y^2\mp 8x^2y^4\mp 64y^6| \end{cases} \tag{19}$$

得到方程

$$2u^4-v^4=w^2 \tag{20}$$

的解。

例如，从方程（16）的解 $x=7$，$y=6$，$z=113$，借助公式（19），得到（20）的解 $u=1525$，$N=1343$，$w=2750257$。

还要指出，方程（20），其中$(u, v)=1$，有无穷多个正整数解 u，v，w。它们依次为（按 x 的值从小到大）：

$x=y=z=1$；$x=13$，$y=1$，$z=239$；$x=$

1525，$y=1343$，$z=2750257$；$x=2165017$，$y=2372159$，$z=3503833734241$；…… 寻找这个方程的解系列的方法是非常复杂的。

（五）n次的方程

这里介绍 $n\geqslant 5$ 次方程解的情况。

1．$\Sigma x_i^5=y^5$

方程

$$x_1^5+x_2^5+\cdots+x_5^5=y^5 \qquad (1)$$

有无穷多整数解，它们可从下列恒等式给出：

$$(75v^5+u^5)^5+(u^5+25v^5)^5+(u^5-25v^5)^5+(10u^3v^2)^5+(50uv^4)^5=(u^5+75v^5)^5 \qquad (2)$$

如果 $0<25v^5<u^5<75v^5$，例如，$u=2$，$v=1$，那么（2）中所有的项都大于零，即有

$$43^5+57^5+7^5+80^5+100^5=107^5.$$

由此求出（1）的一个正整数解。

马丁发现：

$$4^5+5^5+6^5+7^5+9^5+11^5=12^5;$$

$$5^5+10^5+11^5+16^5+19^5+29^5=30^5;$$

$$1^6+2^6+4^6+5^6+7^6+9^6+12^6+13^6$$

$+15^6+16^6+18^6+20^6+21^6+22^6+23^6=28^6$。

2. $ax^m+by^n=cz^p$

容易验证，方程

$$x^3+y^4=z^5 \tag{3}$$

有正整数解 $x=31^5$，$y=31^4$，$z=31^3\times 2$。

一般地，如果 p，q，r 为正整数，并且 pr 与 q 互素，那么方程

$$x^p+y^q=z^r \tag{4}$$

有无穷多正整数解。

证明 由于 $(pr,q)=1$，则存在整数 m，n，使得

$$mq-npr=1$$

设整数 $d\neq 1$，有

$$\begin{aligned}&[(d^r-1)^{nr}]^p+[(d^r-1)^m]^q\\=&(d^r-1)^{npr}[1+(d^r-1)^{mq-npr}]\\=&(d^r-1)^{npr}[1+(d^r-1)]\\=&(d^r-1)^{npr}\cdot d^r=[(d^r-1)^{np}\cdot d]^r\end{aligned}$$

由此得到方程（4）整数解的一种表达式：

$$\begin{cases}x=(d^r-1)^{nr}\\y=(d^r-1)^m\\z=(d^r-1)^{np}\cdot d\end{cases} \tag{5}$$

其中 $d\neq 1$。若（5）中的 d 取不同的整数值，可

得到方程（4）的一些整数解；若取 $d\geqslant 2$，则可得到方程（4）的正整数解。□

现在讨论方程

$$ax^n+by^n=cz^n \tag{6}$$

的整数解情况，其中 a，b，c 是正整数。

我们能够给出一些有整数解的（6）型方程。例如，方程

$$x^3+4y^3=3z^3 \tag{7}$$

有整数解 $x=7$，$y=2$，$z=5$。

方程

$$x^4+34y^4=z^4 \tag{8}$$

有整数解 $x=3$，$y=2$，$z=5$。

然而，我们也可以给出一些没有整数解的（6）型方程。能够证明，如果 $2n+1$ 等于素数 p，$p\mid a$，但 $p^n\nmid a$，$p\nmid b$，$p\nmid c$，$p\nmid(b\pm c)$，那么方程（6）没有整数解。

由此可判断下列方程均无整数解：

$$5x^2+4y^2=3z^2;$$

$$7x^3+23y^3=11z^3;$$

$$11x^5+8y^5=11z^5;$$

$$34x^4+8y^4=z^4;$$

$$23x^{11}+5y^{11}=17z^{11};$$

$$47x^{23}+11y^{23}=z^{23}，等。$$

我们可以做出无穷多个没有整数解的（6）型方程。

3．$x^2 \pm y^2 = z^n$

方程

$$x^2 + y^2 = z^3，(x, y) = 1 \tag{9}$$

的全部正整数解可由下式给出：

$$\begin{cases} x = |r^3 - 3rs^2| \\ y = |3r^2s - s^3| \\ z = r^2 + s^2 \end{cases} \tag{10}$$

其中r，s 是自然数，奇偶性相反，且 $(r, s) = 1$。

事实上，设 $\alpha = r + is \in \mathbf{Z}[i]$，则由棣美弗公式，有

$$|\alpha^3| = |\alpha|^3$$

即

$$(r^3 - 3rs^2)^2 + (3r^2s - s^3)^2 = (r^2 + s^2)^3$$

因而，（10）式确定的 x，y，z 是方程（9）的解。

一般地，如果整数 $n > 1$，那么方程

$$x^2 + y^2 = z^n，(x, y) = 1 \tag{11}$$

的全部正整数解可表示为

$$\begin{cases} x = \left| \frac{1}{2}(\alpha^n + \overline{\alpha}^n) \right| \\ y = \left| \frac{1}{2i}(\alpha^n - \overline{\alpha}^n) \right| \\ z = \alpha\overline{\alpha} \end{cases} \tag{12}$$

其中复整数 $\alpha = r + is$，r，s 是正整数，奇偶性相反，且 $(r, s) = 1$。

或者

$$\begin{cases} x = \left| \sum_{k=0}^{[\frac{n}{2}]} (-1)^k C_n^{2k} r^{n-2k} s^{2k} \right| \\ y = \left| \sum_{k=0}^{[\frac{n-1}{2}]} (-1)^k C_n^{2k+1} r^{n-2k-1} s^{2k+1} \right| \\ z = r^2 + s^2 \end{cases} \tag{13}$$

当 $n = 2$时，（13）成为

$$\begin{cases} x = |r^2 - s^2| \\ y = 2rs \\ z = r^2 + s^2 \end{cases}$$

这正是方程 $x^2 + y^2 = z^2$ 的解。

当 $n = 3$时，（13）成为（10）。

还可用勾股数求方程（11）的解。事实上，设 a，b，c 是一组勾股数，则 ac^{n-1}，bc^{n-1}，c^2 便是(11)的解。直接验证可知

$$(ac^{n-1})^2+(bc^{n-1})^2=(c^2)^n$$

由于勾股数有无穷多，所以(11)也有无穷多个整数解。

方程

$$x^2-y^2=z^3 \tag{14}$$

的整数解可从下列恒等式得到：

$$[r(r^2+3s^2)]^2-[s(3r^2+s)]^2=(r^2-s^2)^3 \tag{15}$$

其中 r，s 为整数。但是，(15)式没有给出(14)的全部整数解。

一般地，当整数 $n\geqslant 2$时，方程

$$x^2-y^2=z^n,\ (x,\ y)=1 \tag{16}$$

的全部整数解可表示如下：

z 是奇数时，

$$\left\{\begin{aligned} x&=\sum_{p=0}^{[\frac{n}{2}]}C_n^{2p}\ a^{n-2p}b^{2p}\\ y&=\sum_{p=0}^{[\frac{n-1}{2}]}C_n^{2p+1}\ a^{n-2p-1}b^{2p+1}\\ z&=a^2-b^2\end{aligned}\right. \tag{17}$$

z 是偶数时，

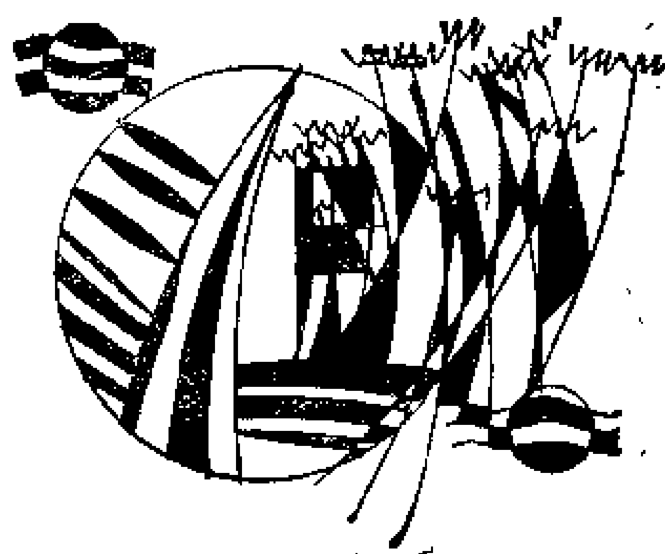
$$\begin{cases} x = 2^{n-2}a^n + b^n \\ y = 2^{n-2}a^n - b^n \\ z = 2ab \end{cases} \tag{18}$$

和

$$\begin{cases} x = a^n + 2^{n-2}b^n \\ y = a^n - 2^{n-2}b^n \\ z = 2ab \end{cases} \tag{19}$$

(17)，(18)和(19)中的 a，b 是自然数，并且 $(a, b) = 1$。

结 束 语



在本书即将结束之际，向青少年读者谈几点看法。

首先，研究 FLT 要先打好基础。

据我们了解，目前有不少数学爱好者在搞 FLT，有的人还把他们的“证明”写成论文，请专家审查或者投给数学杂志。这些稿子大部分是运用整数的整除性和一些初等数论知识，也有的人甚至连这些知识都没用，仅仅用中学课本中的二项式公式，就给出了“证明”。这些证明毫无例外都是错误的。这使我们联想起本世纪初那股热潮，那时有些人的做法现在还在延续。这些同志不了解 FLT 的历史，也不了解 FLT 的困难程度。通过本书的介绍，读者对这些方面会有概括了解。

我们认为，如果有人想从事 FLT 的研究，

打好基础是重要的，就是说，要学习一些必要的数学基础知识，钻研许多有关资料，然后才可进行这方面工作。只用整数的整除性理论和初等数论方法解决问题，那是远远不够的。当然，初等方法也能创造出很高的技巧，并且至今还能用来解决一些困难问题，但是，三百多年的历史告诉我们，FLT不属于这样的问题。关于这个意见，国内外许多著名数学家都有过论述。陈景润说："我认为在最近几十年，关于哥德巴赫猜想、费马大定理等世界著名难题是不能只用初等数论的方法而得到证明的。所以希望青少年同志们不要走入歧途，不要浪费时间和精力。"苏联数学家盖依芳德说："数学爱好者要想用完全初等的方法去证明费马大定理注定不会成功的。"这些忠告是先辈用血汗和生命换来的，值得我们牢牢记取。

在这里，我们要给数学爱好者"泼冷水"。下面介绍数论史上一个掌故，它对同志们会有一定启迪的。据说，希尔伯特的一个学生，有一次写了一篇关于费马大定理的论文，一天晚上他对希尔伯特说："我已经证明了费马大定理，请老师看一看我的论文。"希尔伯特回答说："哦！你可能太疲倦了，需要好好休息一下，明天再来

找我。”第二天，这个学生又去找希尔伯特，他说：“我已经发现昨天的证明是错误的。”

我们不赞成那些没有一定的数学修养的人去搞 FLT.那种“试一试”和“碰碰看”的想法和做法都是不可取的，因为这样做只能是浪费宝贵的时光。我们希望这些同志把时间和精力用在打好基础上，或者选择那些力所能及、四化建设又急需的题目上，这样对现在和将来都是有好处的。

其次，解决 FLT 要有锲而不舍精神。

FLT难度很大，解决它非一朝一夕之功，而要有锲而不舍精神. 陈景润能在哥德巴赫猜想上作出杰出的贡献，与他有锲而不舍精神密切相关. 他在中学时期听到老师讲述哥德巴赫猜想后，立志去研究它. 在以后的几十年的大学学习和科研工作中，他以坚韧不拔的毅力，刻苦研读文献，继承前人的结果并加以创造，取得了巨大成就. 在 FLT 的研究上，这样的例子也是很多的. 早期的库麦潜心研究二十余载，创立了理想数，对 FLT 的研究起了很大推动作用。近代的范迪弗，从本世纪初到五十年代，毕生从事FLT的研究工作，取得了许多重要成果。

最后，我们坚信 FLT 会得到最后解决的。

希尔伯特有句名言："在数学中没有不可知！"无论 FLT 在我们看来多么难以解决，也无论在 FLT 面前我们显得多么无能为力，然而，我们并不悲观．我们坚信，它迟早会得到最后解决的．我们把希望寄托在青年一代．有志攀登 FLT 顶峰的青年们，社会主义祖国为你们的学习和工作创造了十分优越的条件，只要你们踏踏实实，坚持不懈，在继承前人已有成果的基础上，将会创造出崭新的数学方法，来回答FLT的挑战．采撷 FLT 这颗明珠的人可能出于你们之中！

让我们用马克思的一句名言来结束本书：

"在科学上是没有平坦大道的．只有在崎岖山路上攀登、不畏劳苦的人，才有希望到达光辉的顶点．"

参 考 文 献

〔1〕梁宗巨，世界数学史简编，辽宁人民出版社，1981。

〔2〕李迪，费尔马在数学上的伟大贡献，数学通报，1965年1月。

〔3〕洪伯阳，关于费尔马猜想，数学通报，1982年第3期。

〔4〕李心灿，杰出的业余数学家费马，数学通报，1985年3月。

〔5〕董张维，费马的最后定理，同上。

〔6〕张卿，妙趣横生的数学难题，天津人民出版社，1980。

〔7〕尹斌庸等，古今数学趣话，四川科学技术出版社，1985。

〔8〕傅钟鹏，数学的魅力，福建科学技术出版社，1985。

〔9〕李学数，数学和数学家的故事，香港广角镜出版社，1980。

〔10〕郭书春，《九章算术》的整数勾股形研究，科技史文集第8辑，上海科学技术出版社。

〔11〕李继闵，刘徽对整勾股数的研究，同上。

〔12〕D·希尔伯特，数学问题，数学史译文集，上海科学技术出版社，1981。

〔13〕C·瑞德，希尔伯特，上海科学技术出版社，1982。

〔14〕华罗庚，数论导引，科学出版社，1979。
〔15〕陈景润，初等数论Ⅰ，科学出版社，1978。
〔16〕闵嗣鹤、严士健，初等数论，人民教育出版社，1983。
〔17〕熊全淹，初等整数论，湖北人民出版社，1982。
〔18〕潘承洞，素数分布与哥德巴赫猜想，山东科学技术出版社，1979。
〔19〕王湘浩等，离散数学，高等教育出版社，1983。
〔20〕柯召、孙琦，谈谈不定方程，上海教育出版社，1980。
〔21〕柯召、孙琦，关于费马大定理，自然杂志，1980年3卷7期。
〔22〕徐韫和，毕达可拉士定理及福尔玛问题，商务印书馆。
〔23〕M·克莱因，古今数学思想，第3册，上海科学技术出版社，1979。
〔24〕汤健儿，$n=3$时的费尔马问题，数学通报，1965年2月。
〔25〕张禾瑞，近世代数基础，人民教育出版社，1978。
〔26〕李国伟，Hilbert 第十问题，徐氏基金会出版。
〔27〕S. Bloch，Mordell 猜想的证明，数学译林，1985年第四卷第二期。
〔28〕郑格于，勾股定理的推广，数学通报，1964年9月。
〔29〕别莱利曼，趣味代数学，中国青年出版社，1980。
〔30〕孙琦、丢番图方程研究中的某些方法，数理化信息第二辑辽宁教育出版社，1986年。

〔31〕L. E. Dickson, History of the Theory of Numbers Ⅱ, New York, 1971.
〔32〕D. Shanks, Solved and Unsolved Problems in Number Theory, Vol. 1.
〔33〕P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer—Verlag, 1979.
〔34〕H. M. Edwards, Fermat's Last Theorem, 同上.
〔35〕В. Серпинский, О решении, Уравнений в целых гислах, фм, 1961.

中外人名对照

（按笔划多少排列）

三 划

大卫斯	Davis
土厄	Thue
土然	Turán
夕宾斯基	Серинский
马丁	Martin
马其雅谢维奇	Матиясевич
马斯寿泰斯	Massouties

四 划

贝西	Bessy
贝克	Baker
贝努利(1654—1705)	Bernoulli, Jacob
内斯涛德	Nastold
牛顿(1642—1727)	Newton
巴切(1581—1638)	Bachet
巴罗	Barlow
瓦格斯塔夫	Wagstaff

五 划

兰哥文	Langevin
兰道(1877—1938)	Landau
本兹	Bendz
卡利兹	Carlitz
卡绍	Cacho
卡塔兰	Catalan
外斐力什	Wieferich
尼可	Nicol
台特	Tate

六 划

刘维尔(1809—1882)	Liouville
米里曼诺夫(1861—1945)	Mirimanoff
毕达哥拉斯(公元前582—497)	Pythagoras
伐尔廷斯(1954—)	Faltings
色克	Scherk
丢番图(246—330)	Diophantus
约翰逊	Johnson
西格尔	Siegel

七 划

沙尔(1793—1880)	Chasles
辛宰尔	Schinzel
沙伐尔维奇	Shafarevich
库麦(1810—1893)	Kummer
劳	Rao
克罗内克(1823—1891)	Kronecker
克拉斯涅	Krasner
希尔伯特(1862—1943)	Hilbert
佛尔夫斯克尔	Wolfskehl
伯传德	Bertrand
狄利克雷(1805—1859)	Dirichlet
利奔波姆	Ribenboim
阿贝尔(1802—1829)	Abel

八 划

波利尔哈特	Brillhart
波劳克	Pollaok
波美	Pomey
波格曼	Bergmann
波奥尔廷	Poorten
波鲁克内	Brückner
迪克森(1874—1954)	Dickson
法奎姆波古	Fauquembergue

欧拉(1707—1783)	Euler
欧几里得 (约公元前330—275)	Euclide
拉梅(1795—1870)	Lamé
林德曼	Lindemann
帕斯卡(1623—1662)	Pascal
罗克斯顿	Loxton
罗思	Roth
罗宾逊	Robinson
罗特凯也维奇	Rotkiewicz
依恩柯利	Inkeri
绍拉	Chowla

九　划

洪保(1795—1850)	Holmboë
威尔(1906—　)	Weil
柯西(1789—1857)	Cauchy
柯别列夫	Kobelev
胡坚迪(？—1000)	al-Khujandi
费马(1601—1665)	Fermat
哈特	Hart

十　划

高斯(1777—1855)	Gauss
海罗	Hyyrö

热尔曼(1776—1831)	Germain
莱布尼茨(1646—1716)	Leibniz
泰第曼	Tijdeman
莫比乌斯(1790—1868)	Möbius
莫利斯玛	Morishima
莫德尔	Mordell
哥德巴赫(1690—1764)	Goldbach
哥德兹海	Goldziher
格鲁耐特	Grünert
特亚尼安	Terjanian
爱德列曼	Adleman
海斯——布朗	Health——Brown

十一划

盖依芳德(1906—1968)	Гельфанд
培利兹	Pérez
菲尔兹	Fields
勒贝格(1875—1941)	Lebesgue
勒让德(1752—1833)	Legendre
梅森(1588—1648)	Mersnne
笛内斯	Dénes
笛卡儿(1596—1650)	Descartes
曼福得	Mumford
爱斯勒	Eichler

十 二 划

温特	Wendt
棣美弗(1667—1754)	De Moivre
谢尔弗力基	Selfridge
斯台瓦特	Stewart
斯维斯塔克	Swistak
惠更斯(1629—1695)	Huygens
惠维兹	Hurwitz

十三划以上

福特翁勒	Furtwängler
雅可比(1804—1851)	Jacobi
雷麦 D. H	D. H. Lehmer
雷麦 E.	E. Lehmer
瑞阿利斯	Réalis
裴利沙斯特利	Perisastri
戴德金(1831—1916)	Dedekind